– вибір суб'єктів тестування має відповідати задачі тесту і має бути пов’язаний на пряму з діяльністю відділу чи конкретного суб’єкта.

На основі профілів, теорії графів та ряду правил та алгоритмів теорії ймовірності, можна побудувати граф залежностей між відділами, де вершинами будуть відділи або співробітники, а ребрам буде виставлена вага залежності від значень отриманих в ході обчислень на основі можливих оцінок виникнення загроз та критичності ресурсів. Даний вид інтерпретації дозволить візуально оцінити взаємозв’язки між відділами чи співробітниками та визначити пріоритетні маршрути в інформаційній системі в цілому.

Підводячи підсумок, істотну роль в мінімізації ризиків та загроз грає розробка і застосування профілів співробітників, що допоможуть кількісно оцінити можливі загрози і розширити можливості існуючої методології HTRA. Таким чином, для інформаційних систем профілі, дозволять не тільки ефективно оцінити загрози і ризики, но і дозволять вигідніше проводити моніторинг діяльності персоналу, отримувати останню і повну інформацію про конкретного співробітника та визначати залежності між співробітниками в кількісній площині.

Формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах

УДК 004.056.53

Тарас Паращук[1], Анна Корченко [2]
Національний авіаційний університет,[1]taras1039@gmail.com,
[2]annakor@ukr.net

В даний час для вирішення проблеми виявлення атак та загроз пов’язаних з людською складовою приділяється багато уваги. Доказом цього можуть бути дослідження та звіти по всім можливим атакам за 2018-2021р. Тому на основі проаналізованих джерел можна зробити висновок про неухильне зростання атак такого виду, та наявність невеликої кількості систем оцінки загроз та ризиків пов’язаних з людським фактором, дозволяє стверджувати, що дана тема є актуальною, обгрунтованою та потребує подальшого дослідження.

Метою даної роботи є створення методу формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах.

Для початкурозглянемо персонал компанії CE працюючих в певний часовий проміжок t в компанії, тобто:

$$CE^t = \{\bigcup_{i=1}^{n} CE_i^t\} = \{CE_1^t, CE_2^t, \dots, CE_n^t\}, \quad (i = \overline{1,n}) \tag{1}$$

де n визначає кількість всіх співробітників, в певний період часу t.

Далі після сформованої множини CE^t, визначмо множину всі функціональних обов’язків WR, які можуть виникати в процесі функціонування бізнес процесів в певний часовий проміжок t в компанії та можуть бути спільними для декількох співробітників одного відділу або різних, тобто:

$$WR^t = \left\{\bigcup_{i=1}^{n} WR_i^t\right\} = \{WR_1^t, WR_2^t, \dots, WR_n^t\}, \quad (i = \overline{1,n}) \tag{2}$$

де n визначає кількість функціональних обов'язків, що можуть бути у співробітників компанії в певний період часу t.

Визначивши множини для персоналу CE^t та функціональних обов'язків WR^t компанії, визначмо залежність між даними множинами математично, тобто встановимо відповідність. Відповідність між множиною CE^t та WR^t визначимо як кортеж (CE^t, WR^t, ER^t), де CE^t та WR^t — дані множини, між якими встановлюється відповідність, а ER^t— підмножина відповідності.

Підмножину ER^t можна описати графом відповідності (див. рис. 1).

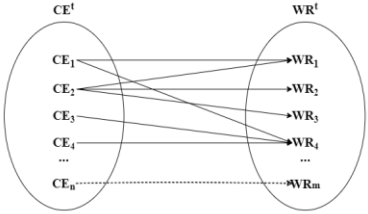

Рис. 1. Граф відповідності між множинами CE^t та WR^t

На основі проілюстрованого графа, маємо що дане відображення є несюр'єктивним та неін'єктивним, тобто кожний елемент WR^t множини асоціюється щонайменше з одним або більше елементів CE^t множини або дані асоціації можуть бути відсутні. Також дану підмножину ER^t можна подати в вигляді:

$$ER^t = \left\{\bigcup_{i=1}^{n}\bigcup_{j=1}^{m}\left(CE_i^t, WR_j^t\right)\right\} = \begin{Bmatrix} (CE_1^t, WR_1^t), (CE_1^t, WR_4^t), \\ (CE_2^t, WR_1^t), (CE_2^t, WR_2^t), \\ (CE_2^t, WR_3^t), (CE_3^t, WR_4^t), \\ (CE_4^t, WR_4^t), \\ \dots \\ (CE_n^t, WR_m^t) \end{Bmatrix}, \quad (3)$$
$$\left(i = \overline{1,n}\right), \left(j = \overline{1,m}\right)$$

де n визначає кількість всіх співробітників та m визначає кількість всіх функціональних обов'язків в компанії.

Проаналізувавши вище описанні відношення та математичні залежності, можна стверджувати що кожному співробітнику може відповідати декілька функціональних обов'язків. Також один функціональний обов'язок може мати відношення до декількох співробітників одночасно.

Описавши залежності вище, перейдемо до визначення та описання загальних параметрів функціональних обов'язків. Для цього опишемо в загальному виді обов'язок WR_i^t з формули (7), за допомогою кортежу з параметрами:

$$WR_i^t = \langle WR_i, PR_i, FPR_i, LC_i, DDR_i \rangle \quad (4)$$

в якому:

- PR_i – пріоритет показує ступень важливості обов'язку в структурі бізнес процесів компанії (шкала оцінки від 1 до 10);

- FPR_i – частота виконання певного обов'язку відносно всіх обов'язків конкретного профілю (шкала оцінки від «рідко» до «дуже часто»);
- LC_i – рівень компетентності конкретного співробітника (профілю) для виконання певного обов'язку (шкала оцінки від «дуже низький» до «високий»);
- DDR_i – ступінь залежності обов'язку від критичних активів та конфіденційної інформації в компанії (шкала від 1 до 10).

Отже, виявлення атак, оцінка загроз та ризиків в соціотехнічних системах є важливим питанням, особливо з точки зору людської складової. Тому розглянутий метод формування параметрів для функціональних обов'язків є важливим етапом при формуванні методології профілювання співробітників певної компанії. Даний метод дозволяє оцінити функціональні обов'язки конкретного співробітника та встановити залежності між співробітником та обов'язками за допомогою параметрів.

Актуальні питання створення систем кібербезпеки в Україні

УДК 355.405.1

Владимир Хорошко[1], Юлия Хохлачева[2], Сергій Скворцов[3], Ахмад Аясрах[4], Аблуллах Аль-Далваш[5]

Национальный авиационный университет,

[1]professor va@ukr.net, [2]hohlachova@gmail.com, [3]ssamailer@gmail.com

Кількість деструктивних інцидентів у сфері комп'ютерних та Internet-технологій за період 2015-2021 років збільшилась приблизно у 2,7 рази. На сьогодні триває кібер-війна України з Росією, під час якої Україна перетворилась на тіньовий полігон для російських хакерів. Щомісяця наша держава піддається кібератакам 3000-3500 разів. Саме тому найбільш пріоритетним напрямом керівництво України вважає реформування систем забезпечення кібербезпеки. Це є одним з головних напрямів забезпечення конфіденційності, цілісності та доступності інформації в національних інформаційних ресурсах від кібератак шляхом створення в інформаційно-телекомунікаційних системах (ІТС) комплексних системах захисту інформації з підтвердженою відповідністю.

Враховуючи таке вже зараз у Адміністративному та Кримінальному кодексах України до переліку протиправних дій у кіберпросторі віднесено :

- несанкціоноване втручання в роботу комп'ютерів та ІТС;
- несанкціонований збут або розповсюдження інформації з обмеженим доступом;
- створення та використання шкідливих програмних та технічних засобів ;