$$\left|\nabla S\right| = S_t'^2 + S_q'^2, \tag{7}$$

$$\nabla^2 S = S_{tt}'' + S_{qq}'', \tag{8}$$

$$\det \mathrm{H} = S_{tt}'' S_{qq}'' - S_{tq}''^2, \tag{9}$$

$$\tilde{k} = S_t'^2 S_{qq}'' + S_q'^2 S_{tt}'' - 2S_t' S_q' S_{tq}'', \tag{10}$$

Детектор єдиного масштабу для знаходження структур типу крапель, який реагує на яскраві і темні структури, схожі на краплі, може базуватися на мінімумі і максимумі лапласіанів $\nabla^2 S$. Афінно–коваріантний детектор структур типу крапель, який також реагує на сідла, може бути представлений як максимум і мінімум детермінанта Гессіана (9). Прямолінійний і афінно–коваріантний детектор кутів може бути представлений як максимум і мінімум кривих рівня масштабування (10) для різних порядків сплайн-операторів, залежно від $r = 2,3,\ldots$ в моделі (1).

Запропоновані інваріанти, сукупно з операторами, на кшталт (3)-(5), або низькочастотних фільтрів на основі сплайн-моделі (1.8), можуть бути рекомендовані для визначення особливостей на даних аерозйомки в якості альтернативи операторів на основі двовимірних функцій Гаусса.

Удосконалення методології HTRA за допомогою системи профілювання персоналу

УДК 004.056.53

Тарас Паращук[1], Анна Корченко [2]

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

Визначення та оцінка людського фактору є важливої для будь-якої інформаційної системи в поточних реаліях. Оскільки останні кібератаки показали, що захист поточних систем базується не тільки на впроваджених системах захисту та моніторингу атак, а й на загальній обізнаності персоналу та інформаційній кваліфікації співробітників. Оскільки захист будь-якої системи починається не тільки

з впровадження політики інформаційної безпеки, визначенням відповідальних осіб, документуванні всіх процесів і т.д., але й слід розглядати кожного працівника компанії, як потенційну точку доступу до інформаційної системи в цілому, а також складову системи, яку важко оцінити та задати конкретні границі впливу на частину системи або всю систему в цілому.

Тому однією із задач при розробці алгоритму для покращення системи оцінки ризиків на базі методології гармонізованої оцінки загроз і ризиків (HTRA), є збір статистики та формування профіля співробітника організації, підвищення інформаційної обізнаності працівників для можливості протидії інформаційним загрозам.

Метою роботи є удосконалення системи на базі HTRA, для розширення можливостей системи по визначенню і оцінці ризиків та загроз, що орієнтовані на співробітника, як найбільш вразливу ланку інформаційної безпеки в цілому.

Опорною складовою, що дозволить розширити оцінку ризиків та загроз, існуючих в оцінюваній системі, пов'язаних зі персоналом є профіль конкретного співробітника. Будь-який профіль співробітника складається з таких блоків:

1. Інформаційний блок:
   - загальна частина (включає в себе загальну інформацію про особу, про посаду, спеціальність, кількість підлеглих, професійні вміння та знання і т.д.);
   - специфічна частина профіля залежно від відділу/професійної спеціалізації/посади.
2. Блок кількісних оцінок (включає в себе оцінки за пройдені тести, так детальну інформацію про формування коефіцієнтів та залежностей між вхідними параметрами).

Інформаційний блок складається з описаних положень, з визначеними ступенями (коефіцієнтами), які можуть бути визначенні алгоритмом або експертом. Ступень важливості певного критерію при подальшій оцінці профілю є певним коефіцієнтом, який може впливати на кінчену оцінку профілю та при побудові ланцюгів ймовірності проведення атаки, з використанням даного співробітника чи групи співробітників.

Блок кількісних оцінок не тільки дозволяє описати кількісно кожен із критеріїв визначених в інформаційному блоці, але і відповідає за відображення всіх розрахованих параметрів (отриманих на основі оцінок інформаційного блоку та системою тестування), що будуть використовуватись в визначенні ймовірності реалізації атаки.

Система тестування може бути визначена за допомогою блоку питань сформованих експертом або специфічних тестів, які мають за собою інформаційну складову (наприклад, лист з вкладенням з програмною закладкою для подальшого отримання до робочої станції). При проведенні будь-якого тестування, для оцінки профілю, необхідно використовувати такий ряд правил:

- тест має мати сформовану задачу, цільову групу співробітників, перелік застосованого обладнання чи програмного забезпечення, кінцеву мету та строго визначений результат;
- оцінки отримані в результаті тестування повинні впливати на профіль співробітника та на відділ;

– 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:

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