ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет безопасности информационных технологий

Дисциплина:

Теория информационной безопасности и методологии защиты информации.

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Выполнил:

Студент гр. N3249

Шарифуллин Ильдан Айдарович

Проверил:

Якимова Софья Андреевна

Санкт-Петербург

2022г.

Лабораторная работа №3

Экспертные оценки

1) ознакомится с материалом

2) составить три задачи в которых (1 - на непосредственную оценку, 2 - на ранжирование, 3 - на ваш выбор):

2.1) приведено условие (ситуация в области ИБ, которую нужно оценить)

2.2) описана анкета (5 вопросов о ситуации/организации/угрозах для экспертов, на которые нужно будет потом ответить)

2.3) описаны веса вопросов анкеты (важность вопросов для оценки)

2.4) подробно описан метод экспертной оценки, который нужно применить и почему для такой ситуации применяется этот метод

2.5) необходимо оценить согласованность мнений экспертов: описать, какой метод оценки применяется, формула, пояснения к формуле (1 - коэф. вариации, 2 - коэф. конкордации, 3 - topsis, 4 - на ваш выбор).

3) привести эталонное (ожидаемое) решение.

Ход работы:

Задача 1:

1. В одной организации поручили реализовать систему удаленного доступа для сотрудников службы поддержи. Из-за слишком маленьких сроков ни о какой комплексной, полноценной системе речь не идет. Поэтому экспертам предлагается попарное сравнение эффективности различных базовых реализаций удаленного доступа.

2. 1) УД стандартными средствами Windows.

   2) Удаленный сервер Ubuntu с разделением пользователей и доступу к БД клиентов.

   3) Сервер с мало проработанной клиентской частью в виде сайта, где после ввода выданных логина и пароля будет реализован доступ к ДБ.

   4) Установка Python скрипта на компьютер каждого сотрудника, при запуске которого будет выводится ДБ клиентов

3. Веса всех вопросов равнозначны

4. Здесь применим метод попарных сравнений, поскольку существенной разницы в значимости факторов нет, при этом требуется выделить 1 наиболее приоритетный.

5. Вычислим коэф. конкордации, поскольку необходимо выяснить согласованность экспертов по выбору наиболее приоритетного критерия.

Результаты:

В таблице под знаком + обозначено превосходство параметра из строки над параметром из столбца, под = их равенство.

Каждая таблица соответствует каждому эксперту:

	У1	У2	У3	У4	Балл	Ранг
У1		=	+	+	2,5	1
У2	=		=	+	2	3
У3	+	=		+	2,5	1
У4	-	-	-		0	4

	У1	У2	У3	У4	Балл	Ранг
У1		-	+	+	2	3
У2	+		=	+	2,5	1
У3	+	=		+	2,5	1
У4	-	-	-		0	4

	У1	У2	У3	У4	Балл	Ранг
У1		+	+	+	3	1
У2	-		+	+	2	2
У3	-	-		+	1	3
У4	-	-	-		0	4

	У1	У2	У3	У4	Балл	Ранг
У1		+	+	+	3	1
У2	-		-	=	0,5	3
У3	-	+		+	2	2
У4	-	=	-		0,5	3

Так как в матрице имеются связанные ранги (одинаковый ранговый номер) в оценках 1-го эксперта, произведем их переформирование. Переформирование рангов производиться без изменения мнения эксперта, то есть между ранговыми номерами должны сохраниться соответствующие соотношения (больше, меньше или равно).

Номера мест в упорядоченном ряду	Расположение факторов по оценке эксперта	Новые ранги
1	1	1.5
2	1	1.5
3	3	3
4	4	4

Номера мест в упорядоченном ряду	Расположение факторов по оценке эксперта	Новые ранги
1	1	1.5
2	1	1.5
3	3	3
4	4	4

Номера мест в упорядоченном ряду	Расположение факторов по оценке эксперта	Новые ранги
1	1	1
2	2	2
3	3	3.5
4	3	3.5

На основании переформирования рангов строится новая матрица рангов.

№ п.п. / Эксперты	1	2	3	4
1	1.5	3	1	1
2	3	1.5	2	3.5
3	1.5	1.5	3	2
4	4	4	4	3.5

Факторы / Эксперты	1	2	3	4	Сумма рангов	d	d^2
x_1	1.5	3	1	1	6.5	-3.5	12.25
x_2	3	1.5	2	3.5	10	0	0
x_3	1.5	1.5	3	2	8	-2	4
x_4	4	4	4	3.5	15.5	5.5	30.25
$\sum$	10	10	10	10	40		46.5

Расположение факторов по значимости

Факторы	Сумма рангов
x_1	6.5
x_3	8
x_2	10
x_4	15.5

$$W = \frac{46.5}{\frac{1}{12} \cdot 4^2(4^3-4)-4 \cdot 1.5} = 0.63$$

W = 0.63 говорит о наличии средней степени согласованности мнений экспертов.

Ожидаемое решение:

У1	У2	У3	У4
6.5	10	8	15.5

Вывод:

Учитывая среднюю степень согласованности предпочтение будет отдано стандартным средствам Windows для реализации УД.

Задача 2:

1. В результате проведения пентеста мультиплатформенной игры независимой группой специалистов было выявлено несколько уязвимостей. Специалистом предлагается оценить потенциальный размер ущерба при эксплуатации каждой из них для определения того, какие уязвимости нужно закрыть максимально срочно.

2. 1) Возможность использовать украденные карты для осуществления доната (CVC обход).

   2) Возможность подмены текстур на всех локациях игры.

   3) Возможность получения прав администратора на серверах игры.

   4) Возможность DOS атаки серверов игры.

   5) Возможность получения доступа к исходному коду игры.

3. Веса всех вопросов равнозначны

4. Здесь применим метод непосредственной оценки, поскольку одинаково важно как ранжировать элементы, так и определить, насколько один элемент важнее других. Возьмем оценки каждого эксперта от 0 до 10, а далее нормируем их сумму для каждого фактора также по шкале от 0 до 10.

5. Вычислим коэф. вариации, поскольку нам важно понимать согласованность по каждому отдельно взятому фактору

Результаты:

	У1	У2	У3	У4	У5
Эксперт 1	10	5	8	10	10
Эксперт 2	10	7	8	9	9
Эксперт 3	10	6	8	10	10
Эксперт 4	8	7	8	8	10
Эксперт 5	9	8	8	9	10
Сумма	47	33	40	46	49
Среднее	9,4	6,6	8	9,2	9,8
СКО	0,8	1,019804	0	0,748331	0,4
Соглас-ть	0,085106	0,154516	0	0,08134	0,040816

Ожидаемое решение:

У1	У2	У3	У4	У5
9	6	8	9	10

Вывод:

Уязвимость №5 обладает наибольшей оценкой при отличной степени согласованности, из-за чего получает первый приоритет. Уязвимости №1 и №4 обладают одинаковой оценкой, при этом согласованность по четвертой превосходит первую. Поэтому приоритеты расставятся так: 5 -> 4 -> 1 -> 3 -> 2.

При этом оценка первых трех сильно превосходит оценку последних двух, поэтому в первом патче стоит закрыть их, а далее работать над закрытием остальных уязвимостей.

Задача 3:

1. В результате проведения закрытого багбаунти одного веб-сервиса, компанией было получено несколько угроз от участников. Требуется распределить места по уровню этих угроз для того, чтобы выплатить справедливые награды нашедшим.

2. 1) sql-инъекция с целью получения ФИО зарегистрированных пользователей

   2) curl запросы для добавления информации на сайт (по-хорошему доступ для этого должен быть только у определенной группы пользователей)

   3) Найдены адреса директорий админ зоны сайта

   4) Возможность сброса пароля другому пользователю (без доступа к новому паролю)

   5) Возможность парсить данные из профилей пользователей в больших объемах. (нет ограничений по количеству запросов)

3. Веса всех вопросов равнозначны

4. Здесь применим метод непосредственной оценки, поскольку важно разместить угрозы в порядке убывания важности.

5. Вычислим коэф. вариации, поскольку нам важно понимать согласованность по каждому отдельно взятому фактору

Результаты:

	У1	У2	У3	У4	У5
Эксперт 1	6	7	8	5	10
Эксперт 2	3	6	8	4	9
Эксперт 3	6	6	8	4	9
Эксперт 4	6	7	8	6	10
Эксперт 5	6	8	8	5	10
Сумма	27	34	40	24	48
Среднее	5,4	6,8	8	4,8	9,6
СКО	1,2	0,748331	0	0,748331	0,489898
Соглас-ть	0,222222	0,110049	0	0,155902	0,051031

Ожидаемое решение:

У1	У2	У3	У4	У5
5	7	8	4	10

Вывод:

Участник, нашедший пятую угрозу, получит наибольшую награду, нашедший третью получит вторую по размеру награду и т.д.