

**Министерство науки и высшего образования Российской Федерации
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 методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

«Экспертные оценки»

Выполнил:

студент группы N3246,

Суханкулиев Мухаммет



(подпись)

Проверила:

Коржук Виктория Михайловна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

Введение	3
1 Ознакомится с материалом	4
1.1 Метод экспертных оценок	4
1.2 Формулы	4
1.2.1 Коэффициент вариации (CV)	4
1.2.2 Стандартное отклонение (σ)	4
1.2.3 Среднее значение (M)	5
2 Задачи	7
2.1 Задача на непосредственную оценку	7
2.1.1 Условие:	7
2.1.2 Анкета:	7
2.1.3 Веса вопросов:	7
2.1.4 Метод экспертной оценки:	7
2.1.5 Оценка согласованности мнений экспертов:	8
2.1.6 Эталонное решение:	8
2.2 Задача на ранжирование	9
2.2.1 Условие:	9
2.2.2 Анкета:	9
2.2.3 Веса вопросов:	9
2.2.4 Метод экспертной оценки:	9
2.2.5 Оценка согласованности мнений экспертов:	10
2.2.6 Эталонное решение:	10
2.3 Задача на попарное сравнение	11
2.3.1 Условие:	11
2.3.2 Анкета:	11
2.3.3 Метод экспертной оценки:	11
2.3.4 Оценка согласованности мнений экспертов:	11
Заключение	12
Список использованных источников	13

ВВЕДЕНИЕ

Цель работы – изучить и научиться применять метод экспертных оценок для анализа информационной безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Ознакомиться с материалом;
2. Разработать и решить три задачи, включающие:
 - Метод непосредственной оценки,
 - Метод ранжирования,
 - Метод на выбор, основанный на конкретной ситуации;
3. Применить соответствующие методы для оценки согласованности мнений экспертов;
4. Привести эталонное (ожидаемое) решение.

1 ОЗНАКОМИТСЯ С МАТЕРИАЛОМ

1.1 Метод экспертных оценок

Метод экспертных оценок используется для анализа ситуаций, где сложно или невозможно получить точные количественные данные. Основные подходы включают:

- **Непосредственная оценка** – эксперты дают свои оценки, которые затем обрабатываются статистическими методами. Применяется для получения мнений по конкретным вопросам.
- **Ранжирование** – каждый эксперт ранжирует предложенные варианты, после чего анализируются средние ранги для выявления наилучшего решения.
- **Попарное сравнение** – варианты сравниваются друг с другом по принципу "лучше-хуже", результатом чего является матрица сравнений.

Для оценки согласованности мнений применяются коэффициенты:

- **Коэффициент вариации (CV)** – показатель разброса оценок относительно среднего.
- **Коэффициент конкордации (W)** – степень согласия в ранжировании вариантов.

Эти методы помогают принимать решения в условиях неопределенности и минимизируют субъективность выбора.

1.2 Формулы

1.2.1 Коэффициент вариации (CV)

Оценивает разброс мнений экспертов относительно средней оценки:

$$CV = \frac{\sigma}{M}$$

Где:

σ – стандартное отклонение,

M – среднее значение.

1.2.2 Стандартное отклонение (σ)

Оценивает степень разброса оценок:

$$\sigma = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (c_i - M)^2}$$

Где:

n — количество оценок;

c_i — оценка эксперта.

1.2.3 Среднее значение (M)

$$M = \frac{1}{n} \sum_{i=1}^n c_i$$

1.2.4 Коэффициент конкордации (W)

Оценивает степень согласованности ранжирования:

$$W = \frac{12S}{d^2(m^3 - m) - d \sum_{s=1}^d T_s}$$

Где:

S — сумма квадратов отклонений;

d — число экспертов;

m — число вариантов;

T_s — корректировка для связанных рангов.

1.2.5 Корректировка для связанных рангов (T_s)

Используется, если в ранжировках есть одинаковые значения:

$$T_s = \sum_{k=1}^{H_s} (h_k^3 - h_k)$$

Где:

H_s — количество групп связанных рангов;

h_k — число связанных рангов в группе.

1.2.6 Сумма квадратов отклонений (S)

$$S = \sum_{j=1}^m (R_j - \bar{R})^2$$

Где:

R_j — средний ранг;

\bar{R} — общее среднее рангов.

1.2.7 Общий ранг варианта

$$r_i = \sum_{j=1}^n r_{ij}$$

Где:

r_{ij} — ранг, присваиваемый j -м экспертом i -му варианту.

1.2.8 Разность ранга

$$d_i = (r_i - \frac{n(m+1)}{2})^2$$

1.2.9 Дисперсия

$$D = \sum_{i=1}^m d_i$$

1.2.10 Максимальная дисперсия

$$D_{max} = \frac{n^2(m^3 - m)}{12}$$

1.2.11 Коэффициент конкордации

$$W = \frac{D}{D_{max}}$$

2 ЗАДАЧИ

2.1 Задача на непосредственную оценку

2.1.1 Условие:

Компания хочет оценить уровень угроз безопасности для своей информационной системы. Для этого она решила провести опрос среди экспертов в области информационной безопасности. Каждый эксперт должен оценить угрозы по пятибалльной шкале, где 1 – незначительная угроза, а 5 – критическая угроза.

2.1.2 Анкета:

- Оцените каждую из угроз по шкале от 1 до 5.
 1. Угроза утечки данных: ____
 2. Угроза кибератак: ____
 3. Угроза внутреннего мошенничества: ____
 4. Угроза использования уязвимостей ПО: ____
 5. Угроза физического доступа: ____

2.1.3 Веса вопросов:

- Угроза утечки данных – 0.2 (высокая важность из-за потенциальных последствий).
- Угроза кибератак – 0.3 (очень важная угроза, поскольку влияет на доступность).
- Угроза внутреннего мошенничества – 0.15 (существенная, но не критическая).
- Угроза использования уязвимостей ПО – 0.25 (высокая вероятность, требует внимания).
- Угроза физического доступа – 0.1 (важно, но менее вероятно).

2.1.4 Метод экспертной оценки:

В данном случае применяется метод непосредственной оценки, так как необходимо собрать мнения экспертов по каждому вопросу. Эксперты предоставляют свои оценки, которые затем обрабатываются статистическими методами, что позволяет получить общее представление о состоянии угроз в компании.

2.1.5 Оценка согласованности мнений экспертов:

Коэффициент вариации позволяет оценить степень разброса мнений экспертов относительно средней оценки. Значение $CV < 0.2$ указывает на достаточную согласованность.

2.1.6 Эталонное решение:

Вопрос	1	2	3	4	5
Вес	0,2	0,3	0,15	0,25	0,1
Эксперт 1	4	5	4	4	3
Эксперт 2	3	4	4	5	3
Эксперт 3	5	5	5	4	3
Эксперт 4	4	5	3	3	2
Эксперт 5	4	4	4	4	3
<i>M</i>	4	4,6	4	4	2,8
σ	0,707107	0,547723	0,707107	0,707107	0,447214
<i>CV</i>	0,176777	0,11907	0,176777	0,176777	0,159719
Взвешенная оценка	0,8	1,38	0,6	1	0,28

Где: Взвешенная оценка = $M \cdot \text{Вес}$

Эталонным решением в данном кейсе будет устранение угроз кибератак.

2.2 Задача на ранжирование

2.2.1 Условие:

Игровая компания провела внутренний аудит безопасности своей игровой платформы и обнаружила несколько потенциальных угроз. Для принятия решения о том, какие угрозы следует устранить в первую очередь, компания решила провести опрос среди экспертов в области информационной безопасности. Эксперты должны ранжировать угрозы по степени критичности, где 1 – незначительная угроза, а 5 – критическая угроза.

2.2.2 Анкета:

Пожалуйста, ранжируйте каждую из угроз по шкале от 1 до 5:

1. Угроза DDoS-атак на игровую платформу: ____
2. Угроза утечки личных данных игроков: ____
3. Угроза использования чит-программ: ____
4. Угроза уязвимостей в игровом коде: ____
5. Угроза фишинга в игровых сообществах: ____

2.2.3 Веса вопросов:

- Угроза DDoS-атак на игровую платформу – 0.25 (очень важная угроза, влияющая на доступность сервисов).
- Угроза утечки личных данных игроков – 0.4 (высокая важность из-за последствий для игроков и репутации компании).
- Угроза использования чит-программ – 0.2 (сильно влияет на игровой баланс, но не критично для безопасности).
- Угроза уязвимостей в игровом коде – 0.1 (требует внимания, но последствия могут быть менее заметными).
- Угроза фишинга в игровых сообществах – 0.05 (менее вероятная угроза, но всё же важна).

2.2.4 Метод экспертной оценки:

В данном случае применяется метод ранжирования, так как необходимо определить приоритеты в устранении угроз. Эксперты ранжируют каждую угрозу, после чего

вычисляется средний ранг для каждого варианта, что позволяет выявить наиболее критичные угрозы.

2.2.5 Оценка согласованности мнений экспертов:

Коэффициент конкордации (W) будет использован для оценки согласованности мнений экспертов при ранжировании угроз. Если значение W близко к 1, это указывает на высокий уровень согласия среди экспертов.

2.2.6 Эталонное решение:

Вопрос	1	2	3	4	5
Вес	0,25	0,4	0,2	0,1	0,05
Эксперт 1	5	4	3	2	1
Эксперт 2	5	4	1	3	2
Эксперт 3	4	5	2	3	1
Эксперт 4	4	5	1	3	2
Эксперт 5	3	5	2	4	1
r	21	23	9	15	7
d	36	64	36	0	64
D	200				
D_{max}	250				
W	0,8				
Взвешенная оценка	1,05	1,84	0,36	0,3	0,07

Эталонное решение будет включать в себя рекомендации по устранению угроз на основе их приоритета, где вверху находятся угрозы, требующие большего внимания:

1. Угроза утечки личных данных игроков;
2. Угроза DDoS-атак на игровую платформу;
3. Угроза использования чит-программ;
4. Угроза уязвимостей в игровом коде;
5. Угроза фишинга в игровых сообществах.

2.3 Задача на попарное сравнение

2.3.1 Условие:

Игровая компания снова проводит аудит своей платформы и хочет уточнить приоритеты устранения угроз, используя метод попарного сравнения.

2.3.2 Анкета:

Эксперты должны заполнить матрицу размером 5×5 , где каждая ячейка a_{ij} будет содержать следующие значения:

- 2, если угроза i предпочтительнее угрозы j (т.е. $i > j$),
- 1, если угрозы i и j равнозначны (т.е. $i = j$),
- 0, если угроза j предпочтительнее угрозы i (т.е. $i < j$).

Пример матрицы:

	DDoS	Утечка	Читы	Уязвимости	Фишинг
DDoS	1	2	2	2	2
Утечка	0	1	1	1	1
Читы	0	0	1	1	1
Уязвимости	0	0	0	1	1
Фишинг	0	0	0	0	1

2.3.3 Метод экспертной оценки:

Метод попарного сравнения заключается в сравнении каждой угрозы с остальными. Эксперты должны заполнить матрицу, в которой указывают, какая угроза важнее, ставя соответствующие оценки. Затем на основе полученных оценок рассчитываются средние ранги для каждой угрозы.

Для вычисления общего ранга каждой угрозы можно суммировать значения в строках матрицы. Каждая строка будет представлять собой угрозу, и сумма будет показывать, насколько она была оценена по сравнению с другими угрозами.

2.3.4 Оценка согласованности мнений экспертов:

Чтобы оценить согласованность мнений экспертов, можно использовать коэффициент конкордации W , как было описано ранее. Формула для его расчета будет аналогична той, что была приведена выше, с учетом среднего ранга и дисперсии.

ЗАКЛЮЧЕНИЕ

Я изучил методы экспертных оценок для анализа угроз информационной безопасности. Применяя методы непосредственной оценки, ранжирования и попарного сравнения, я смог выявить ключевые угрозы.

Полученные знания и навыки будут полезны для дальнейшего развития в области информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. [Microsoft Word - Глава_7.doc \(ifmo.ru\)](#)
2. [Методы экспертных оценок / Хабр \(habr.com\)](#)
3. [ОЦЕНКА СТЕПЕНИ СОГЛАСОВАННОСТИ МНЕНИЙ ЭКСПЕРТОВ | sibac.info](#)
4. [Коэффициент конкордации - Процесс принятия решений в организации \(studbooks.net\)](#)
5. [Коэффициент вариации, формула, пример расчета | Coefficient of Variation \(allfi.biz\)](#)