МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

навчальної дисципліни «**Моделі ризик-орієнтованого аналізу в кібербезпеки**» обов'язкових компонент
освітньої програми другого (магістр) рівня вищої освіти

125 «Кібербезпека» (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.12.2023 № 11

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 20.12.2023 № 11

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 21.12.2023 № 11

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.12.2023 №12)*

Розробник:
Доцент кафедри, к. т. н., доцент Хавіна І.П.

Рецензенти:
1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1. *Вступ до теорії ризиків ІБ.*	10	2			2	6	
Тема № 2. *Технології аналізу ризиків.*	10	2			2	6	
Тема № 3. *Міжнародні стандарти в галузі аналізу та оцінювання ризиків*	16	4			4	8	
Тема № 4. *Методичний підхід до управління ризиками безпеки інформації.*	8	2			2	4	
Тема № 5. *Оцінка ризиків експертними методами.*	14	2			4	8	
Тема № 6. *Метод оцінки ризиків на основі моделі загроз і вразливостей.*	14	4			2	8	
Тема № 7. *Методика аналізу ризиків інформаційної безпеки на основі нечіткої логіки.*	18	4			4	10	
Всього:	**90**	**20**			**20**	**50**	**залік**

1. Методичні вказівки до лабораторних занять

Лабораторна робота № 1

Тема: Аналіз ризиків та основні принципи забезпечення інформаційної безпеки (матричний підхід 1).

Мета роботи:

1. Поглиблення та закріплення теоретичних знання з питань:
- поняття ризиків інформаційної безпеки та їх аналіз;
- основні принципи та методи забезпечення інформаційної безпеки.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1.Ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації.

2.Набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення ІБ.

Висновки.

Література:

1. Матеріали лекції 1.

[1, с. 8 – 12, 16 - 19]

2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Стислі теоретичні відомості

1.1. Поняття ризиків інформаційної безпеки

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерному шахрайству, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз інформаційної безпеки та ймовірності реалізації цих загрози.

В зв'язку з цим, також необхідно володіти таким поняття як ***ризик інформаційної безпеки*** – потенційна можливість використання загрозою вразливостей інформаційного активу або групи активів для заподіяння шкоди об'єктам або інтересам суб'єктів інформаційних відносин. Виходячи з визначення ризику, для проведення аналізу ризиків потрібні наступні дані про інформаційну систему: перелік цінної інформації із зазначенням її рівня критичності, відомості про уразливість інформаційної системи і загрози, які на неї діють.

При цьому необхідно відзначити, що жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки. Саме тому й проводиться аналіз та оцінка ризиків ІБ.

1.2. Аналіз ризиків інформаційної безпеки – матричний підхід

Розрізняють два методи аналізу та оцінки ризиків: ***кількісний*** та ***якісний***.

Для кількісної оцінки ризиків характерне використання об'єктивних чисельних, а саме фінансових характеристик. На відміну від кількісного, якісний аналіз ризиків не ставить своїм завданням отримання чисельних фінансових характеристик. Для оцінки активів і критичність загроз вводиться якісна неформальна або напівформальна шкала, і основною метою такого аналізу стає ранжування загроз відповідно з обраними критеріями.

Оскільки даний курс присвячений основам інформаційній та кібернетичній безпеці, а не менеджменту ІБ, в лабораторній роботі буде розглянуто один із якісних методів аналізу ризиків, а саме матричний підхід аналізу ризиків ІБ, який пов'язує активи, уразливості, загрози та засоби контролю (міри, які організація може прийняти для мінімізації дій загроз на один чи більше активів) і визначає важливість різних засобів контролю, відповідним активам організації.

Матричний підхід використовує три окремих матриці: матрицю уразливостей, матрицю загроз і матрицю засобів контролю, які дозволяють зібрати всі необхідні дані для аналізу ризиків ІБ.

Матриця уразливостей складається із взаємозв'язків між активами і уразливостями в організації, в свою чергу матриця загроз відображає взаємозв'язки між уразливостями і загрозами, а матриця засобів контролю містить взаємозв'язки між загрозами і засобами контролю. Таким чином, кожна клітинка в таблиці відображає значення взаємозв'язку між елементами рядків та стовпців. В даному методі використовується наступна шкала взаємозв'язку (оцінки впливу): немає впливу, слабкий, помірний, сильний вплив.

При первинному аналізі ризиків формуються списки активів, уразливостей, загроз, засобів контролю, які в подальшому додаються до відповідних таблиць. Матриці заповнюються поступово шляхом додавання даних щодо взаємозв'язку елементів стовпця матриці з елементами рядка. Спершу заповнюється матриця уразливостей, дані якої обчислюються за допомогою формули (1.1), для визначення вагомості (значущість) уразливостей, після чого останні переносяться до наступної матриці – матриці загроз. Аналогічно, дані в матриці загроз обчислюються за допомогою формули (1.2), таким чином визначаючи потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці. В результаті чого, формується матриця контролю, яка містить відносну важливість різних засобів контролю. Дана матриця визначає необхідність в застосуванні конкретних мір або засобів захисту для мінімізації впливу загроз на один або більше активів організації зменшуючи рівень ризиків (демонструючи «чистий ризик» – ризик з мінімізованою реалізацією загроз).

Таблиця 1.1. Матриця уразливостей (взаємозв'язок між активами та вразливостями)

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний C_j	**Активи:**	Секрети виробництва	Конфіденційна інформація	Репутація (довіра)	Апаратне забезпечення	Програмне забезпечення	Послуги	Комунікації	**Всього**	**Ранжування**
Уразливості:	РП								Σ	
Веб-сервер										
Обчислювальний сервер										
Міжмережевий екран										
Маршрутизатор										
Клієнтський вузол										
База даних										

Припустимо, що є n активів, де відносна вартість активу $a_j \in C_j$ $(j = 1, \cdots, n)$. Також нехай v_{ij} – це відносний вплив уразливості v_i на актив a_j. Тоді потенційний вплив уразливості V_i на активи організації обчислюється за формулою:

$$V_i = \sum_{j=1}^{n} v_{ij} C_j \qquad 1.1$$

Таблиця 1.2. Матриця загроз (взаємозв'язок між уразливостями та загрозами)

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Веб-сервер	Обчислювальний сервер	Міжмережевий екран	Маршрутизатор	Клієнтський вузол	База даних	Передача даних	**Всього**	**Ранжування**
Загрози:	РП								Σ	
Відмова в обслуговуванні (DoS)										
Шкідливе ПЗ										

Помилки користувача										
Спам										
«Фішинг»										
Ворожий агент										

Припустимо, що існує p загроз, які можуть бути реалізовані за допомогою n уразливостей та t_{ki} – відносна можливість використання загрозою t_k уразливості v_i. Тоді потенційна реалізація конкретної загрози T_k обчислюється за формулою:

$$T_k = \sum_{i=1}^{n} t_{ki} V_i \qquad 1.2$$

Таблиця 1.3. Матриця контролю (взаємозв'язок між загрозами та засобами захисту)

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Відмова в обслуговуванні	Шкідливе ПЗ	Помилки користувача	Спам	«Фішинг»	Ворожий агент	Збій електроживлення	**Всього**	**Ранжування**
Засоби контролю:	РП								Σ	
Система виявлення вторгнень (IDS)										
Навчання персоналу										
Міжмережевий екран										
Політика безпеки										
Конфігурація архітектури мережі										
Демілітаризована зона (DMZ)										

Припустимо, що є q засобів контролю (захисту), які можуть пом'якшити (мінімізувати) вплив p загроз, а z_{lk} – відносний вплив засобу контролю z_l на загрозу t_k. Тоді потенційне пом'якшення загроз за допомогою конкретного засобу контролю – Z_l, обчислюється за формулою:

$$Z_l = \sum_{i=1}^{p} z_{lk} T_k \qquad 1.3$$

Таким чином, за допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби

контролю, в результаті чого ми одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

1.2.1. Приклад використання методики аналізу ризиків ІБ

Дослідження аналізу ризиків за допомогою запропонованої методики буде здійснюватися на прикладі компанії «Cyberstec», яка займається розробкою програмного забезпечення. На даний момент компанія займається розробкою проектів в основному зосереджених в таких областях як: безпека робочих станцій і мережева безпека, віртуалізація та віддалений доступ, управління поведінкою системи, обробка даних, робота з мобільними пристроями. Вона має фрагментовану організаційну структуру, працює у декількох містах України (Київ, Львів, Харків, Одеса), а також має бізнес представництво у місті Мюнхен (Німеччина). Це достатньо конкурентний бізнес, де постійно розвиваються ІТ-технології і виробники постійно намагаються обійти один одного, таким чином, інформаційна безпека – є критичним фактором для захисту активів компанії і запобіганню зриву її діяльності.

Саме тому, для правильної організації системи безпеки, вибору конкретних методів захисту, та планування витрат на ІБ, в компанії проводиться аналіз інформаційних ризиків за допомогою запропонованої методики. Три матриці, які пов’язують активи та уразливості, уразливості та загрози, загрози та засоби контролю, представлені в таблицях 1.4, 1.5 та 1.6 відповідно.

Таким чином, у таблиці 1.4 представлено матрицю уразливостей, яка пов’язує уразливості та активи компанії «Cyberstec». Для побудови матриці була визначена відносна цінність активів та проведено їхнє ранжування (з права на ліво). Наприклад, успішність компанії залежить від її здатності розвивати і захищати нові технології; тому вони високо оцінюються. Ґрунтуючись на активах, було визначено ключові уразливості, надано їм ранг пріоритету та встановлено відносний вплив уразливостей на активи компанії. Так як зовнішні порушники (хакери) спершу повинні обійти брандмауер, щоб отримати доступ до конфіденційної інформації, він займає перше місце у матриці уразливостей. Окрім того, як було зазначено раніше, філії компанії територіально розкидані, тому передача та синхронізація даних також оцінюються високо.

Таблиця 1.1. Матриця уразливостей «Cyberstec»

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний C_j	**Активи:**	Новітні розробки (технології)	Конф. інф. (програмний код)	Репутація (довіра)	Доступність сервісів	Комунікації	Програмне забезпечення	Апаратне забезпечення	**Всього**	**Ранжування**
Уразливості:		7	6	5	4	3	2	1	Σ	
Брандмауер	5	9	9	3	9	9	9	9	222	9
Передача даних та лінії зв'язку	5	9	9	3	9	9	3	9	210	8
Фізична безпека	4	9	9	3	1	1	3	9	154	5
Помилки конфігурації серверів екстранет	4	9	9	1	9	3	9	1	186	7
ПК співробітників компанії	3	3	9	1	0	1	9	3	104	2
Бази даних	4	9	9	3	3	1	9	1	166	6
Стійкість паролів	3	9	9	1	1	3	9	1	154	4
Помилки конфігурації серверів інтернет	2	1	1	9	9	3	9	1	122	3
Ненадійне джерело живлення	1	0	0	3	9	9	0	1	79	1

В результаті, як бачимо, в матриці було проведено обчислення потенційного впливу уразливостей на активи «Cyberstec» за формулою (1.1) для того, щоб відранжувати уразливості і таким чином визначити їхню значущість.

Після цього уразливості були перенесені до наступної матриці.

Беручи до уваги наявні уразливості в активах компанії, було визначено ключові загрози, надано їм ранг пріоритету та аналогічним чином, встановлено відносну можливість використання загрозою уразливості.

Таблиця 1.2. Матриця загроз «Cyberstec»

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Брандмауер	Передача даних та	Помилки конфігурації серверів	Бази даних	Фізична безпека	Стійкість паролів	Помилки конфігурації серверів	ПК співробітників компанії	Ненадійне джерело живлення	**Всього**	**Ранжування**
Загрози:		9	8	7	6	5	4	3	2	1	Σ	
Відмова в обслуговуванні (DoS/DDos)	5	9	9	9	0	1	1	9	1	1	255	5
Шкідливе ПЗ	4	1	1	9	1	1	1	3	9	1	123	2
Помилки працівника	2	1	1	3	3	3	3	3	9	1	111	1
Збої сервера	5	9	9	9	9	9	1	9	1	9	357	8
Вторгнення (атака на пароль)	3	9	3	9	9	1	9	3	3	1	279	6
Фізичне пошкодження ІТС	3	1	9	3	3	9	0	3	3	3	183	3
«Спуфінг» та «Маскарад»	2	1	9	9	3	1	1	9	9	1	217	4
НСД	5	9	3	9	9	9	9	9	9	1	349	7

В результаті обчислень за допомогою формули (1.2), було визначено потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці.

Останньою формується матриця контролю, до якої, окрім загроз, були внесені запропоновані засоби контролю з відповідним рангом пріоритету. Після чого було встановлено відносний вплив засобу контролю на загрозу з використанням суб'єктивних суджень, і обчислено за формулою (1.3) потенційне пом'якшення загроз. Отримані дані були відранжовані з метою визначення пріоритетних засобів контролю. Ця інформація, в поєднанні з вартістю засобів контролю використовується для планування ІБ.

Таким чином, результати аналізу і узагальнення даних, що містяться в матрицях будуть використовуватися під час процесу інтеграції та вибору програмного забезпечення і апаратного устаткування в компанії «Cyberstec».

Таблиця 1.3. Матриця контролю «Cyberstec»

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Збої сервера	НСД	Вторгнення (атака на пароль)	Відмова в обслуговуванні	«Спуфінг» та «Маскарад»	Фізичне пошкодження ІТС	Шкідливе ПЗ	Помилки працівника	**Всього**	**Ранжування**
Засоби контролю:		8	7	6	5	4	3	2	1	Σ	
Система виявлення вторгнень (IDS)	5	9	9	3	9	9	1	3	3	246	6
Навчання персоналу	2	1	0	9	0	3	3	9	9	110	1
Міжмережеві екрани	5	9	9	9	9	9	1	3	1	280	7
Політика безпеки	4	1	9	9	3	9	1	9	3	200	4
Конфігурація архітектури мережі	5	9	3	1	9	1	0	0	1	149	2
Демілітаризована зона (DMZ)	3	9	9	3	9	3	0	0	3	213	5
Контроль території	4	3	9	9	1	1	9	3	1	184	3

1.3. Основні принципи та методи забезпечення інформаційної безпеки

З метою протидії основним загрозам ІБ, система забезпечення інформаційної безпеки ІТС повинна вирішувати наступні завдання:

1) розмежування та контроль доступу користувачів до ресурсів ІТС;

2) захист всіх даних, що передаються по каналах зв'язку;

3) реєстрація, збір, зберігання, обробка і видача інформації про всі події, що відбуваються в системі і мають відношення до забезпечення її безпеки;

4) моніторинг роботи користувачів ІТС системою захисту інформації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

5) забезпечення замкнутого середовища функціонування вже перевіреного ПЗ з метою захисту від неконтрольованого впровадження в систему потенційно небезпечних програм (які можуть містити «закладки» або критичні помилки) і засобів подолання системи захисту, а також від впровадження та поширення шкідливого ПЗ;

6) забезпечення доступності інформаційних ресурсів шляхом резервного копіювання даних;

7) забезпечення та контроль цілісності критичних ресурсів системи захисту ІТС.

Також необхідно відмітити, що розрізняють зовнішню та внутрішню безпеку ІТС. Зовнішня безпека полягає в захисті ІТС від загроз природного походження, а також від проникнення в систему зловмисників ззовні.
Внутрішня ж безпека повинна створювати надійний і зручний механізм регламентування діяльності усіх законних користувачів та обслуговуючого персоналу ІТС, а також забезпечувати цілісність даних.

Що стосується ***методів забезпечення інформаційної безпеки*** то вони достатньо різноманітні, однак їх можна розділити на наступні основні групи: теоретичні, законодавчі (правові), адміністративні (організаційні), інженерно-технічні (програмно-технічні) та криптографічні.

Теоретичні методи забезпечення інформаційної безпеки вирішують два основних завдання. Перше з яких – формалізація різного роду процесів, пов'язаних із забезпеченням інформаційної безпеки. Так, наприклад, формальні моделі управління доступом дозволяють строго описати всі можливі інформаційні потоки в системі – а значить, гарантувати виконання необхідних властивостей безпеки. Звідси безпосередньо випливає друге завдання – суворе обґрунтування коректності і адекватності функціонування систем забезпечення інформаційної безпеки при проведенні аналізу їх захищеності. Така задача виникає, наприклад, при проведенні сертифікації автоматизованих систем за вимогами безпеки інформації.

Законодавчі міри захисту визначаються діючими в країні нормативно-правовими актами, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил. Важливе значення мають стандарти в області захисту інформації (у першу чергу, міжнародні). Серед цих стандартів виділяються «Помаранчева книга», рекомендації X. 800 і «Загальні критерії оцінки безпеки інформаційних технологій».

Адміністративні методи захисту – методи організаційного характеру, які регламентують процеси функціонування ІТС, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою мінімізувати або виключити можливість реалізації загроз безпеки.
Зазвичай вони включають:

- підбір та підготовку персоналу системи;
- організацію охорони та контрольно-пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів та носіїв з інформацією;
- розподіл атрибутів розмежування доступу (паролів, ключів шифрування тощо).

Основою адміністративних методів захисту інформації є формування *політика безпеки* організації – сукупність вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Криптографічні методи захисту інформації реалізується шляхом перетворення інформації (шифрування, кодування та інші перетворення) з використанням спеціальних (ключових) даних та алгоритму зворотного перетворення з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Можна стверджувати, що на теперішній час, криптографічний метод захисту є одним із найбільш надійніших методів захисту, оскільки захищається безпосередньо сама інформація, а не доступ до неї.

Інженерно-технічні методи захисту інформації засновані на використанні спеціальних інженерно-технічних заходів, апаратних засобів і програмного забезпечення, що входять до складу ІТС і унеможливлюють виток, знищення або блокування інформації, порушення цілісності та режиму доступу до неї.

Однак, необхідно відзначити, що універсальних методів захисту не існує, і тому під час вирішення питання щодо захисту інформації потрібно обов'язково враховувати критичність інформаційних активів, усі наявні ризики, а вже потім використовувати конкретні механізми забезпечення безпеки та планувати витрати на ІБ. Багато в чому успіх при побудові механізмів безпеки для реальної системи буде залежати від її індивідуальних особливостей, облік яких погано піддається формалізації. Тому часто інформаційну безпеку розглядають як певну сукупність неформальних рекомендацій щодо побудови систем захисту інформації того чи іншого типу.

Порядок виконання лабораторної роботи №1:

1. Ознайомитися з короткими теоретичними відомостями.
2. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою матричного підходу 1.
3. На основі отриманих результатів, надати основні рекомендації щодо забезпечення ІБ в даній організації.
4. Оформити звіт згідно до вимог.
5. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.

2. Постановка завдання.

3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.

4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.

5. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.

6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.

7. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи № 1

Таблиця № 1.7. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Організація	Кількість інформаційних активів
1	Державний комерційний банк	8
2	Приватна поліклініка	9
3	Страхова компанія	7
4	Інтернет-магазин	9
5	Адвокатська контора	8
6	Агентство нерухомості	7
7	Рекламне агентство	7
8	Науково-проектне підприємство	9
9	Аудиторська компанія	8
10	Туристичне агентство	7
11	Консалтингова фірма	9
12	Фармакологічна компанія	8
13	Архітектурне агентство	7
14	Інтернет-провайдер	7
15	Будівельна компанія	8
16	Система електронних платежів	9
17	Видавництво	7
18	Благодійний фонд	8
19	Рекрутингове агентство	7

20	Міжнародний комерційний банк	9
21	Військове підприємство	6
22	Компанія-розробник ПЗ	9
23	Дизайнерська фірма	8
24	Організація з розробки електроніки	9
25	Державна поліклініка	8
26	Авіакомпанія	9
27	Редакція газети	7

Контрольні питання

1. Надати визначення наступним поняттям: ризик ІБ.
2. Коротко описати алгоритм аналізу ризиків інформаційної безпеки організації.
3. Які повинна вирішувати завдання система забезпечення інформаційної безпеки ІТС?
4. Коротко охарактеризувати основні групи методів забезпечення ІБ.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. 1. Goel, S., Chen, V. Information security risk assessment – a matrixbased approach. University at Albany. – SUNY. – 2005.

Додаткова література з навчальної дисципліни

5. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

6. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

7. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

8. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

9. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

10. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

11. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 2

Тема: Дослідження якісної оцінки ризиків ІБ з урахування додержання норм, організації та технічного забезпечення підприємства (матричний підхід 2).

Мета роботи: комп'ютерне моделювання ІБ за допомогою засобів Excel.

Придбання та опанування практичних навичок з аналізу та якісної оцінки ризиків ІБ підприємства.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Список активів організації.
2. Матриця вразливостей та загроз.
3. Матриця контролю.
4. Шкала ранжування.
5. Оцінка цінностей компанії
6. Аналіз організаційних заходів захисту інформації.
7. Ймовірність реалізації актуальних загроз
8. Аналіз технічних заходів захисту інформації
9. Ризики реалізації загроз інформаційній безпеці для активів.

Висновок.

Література:

1. Матеріали лекції 2.

[2, с. 5 - 9]

2. Нормативні документи [1].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Intertnet.

Заняття проводиться в комп'ютерному класі. Кожний студент забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити питання оцінки ризиків організації та функціонування систем технічного захисту інформації.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Хід роботи

Порядок виконання лабораторної роботи №2:

6. Ознайомитися з короткими теоретичними відомостями.
7. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою матричного підходу 2.
8. Заповнити даними, згідно свого варіанту та провести розрахунки у табл. 3.1 – 3.12
9. На основі отриманих результатів, надати основні рекомендації щодо оцінки ризиків та забезпечення ІБ в даній організації.
10. Оформити звіт згідно до вимог.
11. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.
4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені матриці.
6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.
7. Висновки та відповіді на контрольні питання.

Теоретичні відомості

За допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті

чого одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації.

Виконувати комп'ютерне моделювання ІБ за допомогою засобів Excel.

Проведемо оцінку. На першому етапі «Ідентифікація активів» - сформуємо список активів організації. Процес збору адміністратором інформаційної безпеки даних для аналізу ризиків, відбувався шляхом опитування співробітників підприємства. В якість активів: персональні дані, комерційна таємниця, електронні документи, електронна пошта, АРМ, бази даних, сервер.

Таким чином, було сформовано (при зборі даних для аналізу ризиків за матричною методологією) три матриці: матрицю вразливостей (містить зв'язок між активами і слабкими місцями в організації)(табл. .3.1), матрицю загроз (відношення між слабкими місцями та загрозами) (табл. .3.2), матрицю контролю (зв'язки між загрозами та засобами керування) (табл. .3.3).

Значення кожної клітинки матриці показує оцінку відношення між елементом рядка і стовпця. В основному, використовують таку систему оцінок, як «низька», «середня» і «висока».

При формуванні номенклатури активів, слабких місць та загроз, було використано наступну шкалу оцінки взаємо залежностей активів (загроз) і слабких місць (вразливостей):

0 – немає впливу;

1 – слабкий вплив;

3 – помірний вплив;

9 – сильний вплив.

Ранжування пріоритету вразливостей проведено за наступною шкалою:

1 і 2– неважлива;

3– важлива, але не ключова;

4– важлива, але знаходиться під впливом ключової;

5– ключова.

Отже, отримані матриці активів та загроз ТОВ наведені у таблицях 3.1–3.6.

Таблиця 3.1 Матриця активів

Матриця активів	Загрози	Шкідливе програм забезпечення	Хакерські атаки	Втрата інформації (вірус)	Персонал	Пожежа	Всього	Розряд
Уразливості, пріоритет		**5**	**4**	**3**	**2**	**1**		
Локальна мережа	5	3	3	3	0	0	36	2
База даних (БД)	4	9	3	9	0	0	84	4
Передача даних через інтернет	5	9	9	9	9	9	129	5
Перерва в подачі енергії	2	1	1	3	1	9	29	1
Апаратно-програмні збої	3	3	3	9	3	9	69	3
Людський фактор (помилки користувача)	5	9	9	9	9	9	135	6

Таблиця 3.2 Матриця загроз

Матриця загроз	Уразливості	Людський фарктор	Передача данних через Інтернет	Бази даних	Апаратно-програмні сбої	Локальна мережа	Перерва з подачі енергії	Всього	Розподіл
Уразливості, пріоритет		**6**	**5**	**4**	**3**	**2**	**1**		
Шкідливе програмне забезпечення	**4**	9	9	9	9	3	0	168	**5**
Втрата інформації (вірус)	**3**	9	9	9	3	1	0	146	**3**

Хакерські атаки (перехоплення, спотворення, знищення, підміна маршрутів слідування інформації)	**4**	9	9	9	0	0	0	135	**4**
Персонал	**5**	9	3	3	3	3	3	99	**2**
Пожежа	**2**	1	0	0	0	1	3	11	**1**

Сукупні дані про погрози і відповідні засоби управління додаються в матрицю контролю, представлену в таблиці 3.3

Таблиця 3.3 Матриця контролю

Матриця контролю	Загрози	Шкідливе програмне забезпечення	Хакерські атаки	Втрата інформації (вірус)	Персонал	Пожежа	Всього	Розподіл
Управлінські дії, пріоритет		**5**	**4**	**3**	**2**	**1**		
Використання ліцензійного ПЗ	**5**	9	1	1	1	0	54	**5**
Електронний цифровий підпис	**5**	0	9	1	9	0	57	**6**
Антивірусне ПЗ	**4**	0	0	3	9	0	27	**3**
Трудовий договір з пунктом про нерозголошення інформації	**4**	0	0	3	9	0	27	**3**
Парольний захист на ресурси	**5**	0	3	0	9	0	30	**4**
Маршрутизатор (роутер)	**3**	0	3	3	0	0	21	**2**
Протипожежна сигналізація	**3**	0	0	0	0	9	9	**1**

На другому етапі «Визначення ризиків невідповідності законодавству в області інформаційної безпеки». Присвоюється значення «1», якщо немає,

то – «0». Всі вимоги, яким присвоєно значення «1», підсумовуються, інші значення не враховуються (табл. 3.4).

Отже, рівень ризику невідповідності вимогам до інформаційної безпеки становить $R_n = 0,25$ (табл. 3.5).

Таблиця 3.4 Ризик невідповідності законодавству в області інформаційної безпеки

	Вимоги законодавства	Виконання вимог
1	Реєстрація в якості оператора персональних даних	1
2	Розробка і прийняття документів, що регламентують питання надання доступу і захист персональних даних	1
3	Оформлення допусків співробітників до персональних даних	0
4	Формування переліку оброблюваних персональних даних	1
5	Класифікація інформаційної системи обробки персональних даних	1
6	Підготовка інформаційної системи обробки персональних даних до атестації за вимогами безпеки	1
7	Вживання заходів щодо захисту персональних даних	1
8	Сертифікація системи захисту інформації у складі інформаційної системи обробки персональних даних	0
9	Сертифікація заходів системи захисту інформації у складі інформаційної системи обробки персональних даних	1
10	Встановлення вимог до надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
11	Перевірка на відповідність вимогам надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
12	Введення обмежень на придбання і використання окремих видів апаратних і програмних засобів в інформаційній системі	0
13	Технічні (в т.ч. програмні) засоби обмеження доступу в інформаційних системах не створювати загрозу або завдавати шкоди здоров'ю і майну інших осіб	1

14	Обов'язок щодо забезпечення конфіденційності відомостей, що становлять професійну таємницю	1
	Всього	11

Таблиця 3.5 Значення ризику невідповідності вимогам законодавства

Сума виконаних вимог	Ризик невідповідності вимогам законодавств
13–14	0,01
8–12	0,25
Менше або рівне 7	0,5
Не виконуються	0,9

На наступному етапі розробляється модель загроз. Визначається ймовірність виникнення несприятливих подій і актуальність загроз інформаційної безпеки. По завершенню етапу формується список актуальних загроз на кожен актив або групу активів.

Таким чином, для ТОВє наступний список актуальних загроз: шкідливе програмне забезпечення, втрата інформації через віруси, пожежа, персонал, хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування інформації).

На останньому етапі – проводиться кількісна оцінка ризиків. Для цього:

1) обираються актуальні загрози – за допомогою моделі загроз складається список актуальних загроз. Ідентифіковані активи зіставляються з спрямованими на них погрозами;
2) визначаються ймовірності виникнення загроз. При цьому, на один актив можуть впливати одночасно декілька загроз. Тому, слід з'ясувати ймовірність того, що хоча б одна загроза реалізується по відношенню до заданого активу.

Ймовірність реалізації хоча б однієї загрози з сукупності ймовірностей загроз $y_1, y_2, \ldots y_n$, де n – кількість загроз, дорівнює різниці між одиницею і добутком ймовірностей протилежних подій.

Отже, маємо наступні ймовірності реалізації актуальних загроз – таблиця 3.6.

Таблиця 3.6 Ймовірність реалізації актуальних загроз

Загроза інформаційній безпеці	Значення ймовірності реалізації загроз
Шкідливе програмне забезпечення	0,3
Втрата інформації через віруси	0,45
Пожежа	0,1
Персонал	0,75
Хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування інформації)	0,65

Ймовірність реалізації хоча б однієї загрози зі списку актуальних загроз $R_{угр} = 0,9934$;

3) визначаються цінності активів – ця величина знаходиться в діапазоні від 0 до 1 (показує відношення ціни активів до вартості всього бізнесу). Визначену оцінку представлено у таблиці 3.7;

4) визначаються можливості застосування організаційних і технічних вразливостей. Ймовірність застосування організаційних вразливостей проводиться експертними методом. В процесі виконання аналізу всіх організаційних заходів, виконуваних, присвоюється значення «1», а тим, що не виконуються «0». Аналіз організаційних заходів захисту інформації наведені у таблиці 3.8;

Таблиця 3.7 Оцінка цінностей компанії

Назва активу	Значення оцінки цінностей активу
Персональні данні	0,7
Комерційна таємниця	0,6
Електронні документи	0,55
Електронна пошта	0,5
АРМ	0,35
Бази даних	0,4
Сервер	0,45

Таблиця 3.8 Аналіз організаційних заходів захисту інформації

Організаційні заходи захисту інформації	Оцінка виконання організаційних заходів щодо захисту інформації
Організаційна інфраструктура інформаційної безпеки	1
Координація питань інформаційної безпеки	1
Розподіл обов'язків по забезпеченню інформаційної безпеки	1
Призначення відповідальних за кожен актив або процедуру безпеки	0
Отримання доступу до засобів обробки інформації з боку керівництва та адміністраторів засобів управління	1
Перевірка сумісності з іншим програмним забезпеченням і компонентами системи апаратних засобів	1
Співпраця організацій в області інформаційної безпеки	1
Незалежна перевірка (аудит) інформаційної безпеки	0
Включення вимог безпеки до договорів зі сторонніми особами та організаціями	0
Залучення сторонніх організацій до обробки інформації (Аутсорсинг)	0
Включення вимог безпеки за договором на аутсорсинг	0
Облік активів	1
Інвентаризація активів	1
Класифікація інформації	1
Облік питань безпеки в посадові обов'язки і при прийомі на роботу персоналу	1
Навчання користувачів	1
Контроль доступу до зони контролю	1
Управління передачею даних і операційною діяльністю	1
Безпека електронної пошти	0
Контроль доступу до інформації	1
Управління безперервністю бізнесу	0

Всього	14

Таким чином (табл. 3.9), коефіцієнт уразливості організаційних заходів захисту K_o = 0,01.

Таблиця 3.9 Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості організаційних заходів захисту
14–17	0,01
9–13	0,25
Менше або рівне 8	0,5
Не виконуються	0,9

Оцінка технічних вразливостей проведено експертним методом, в ході якого були проаналізовані технічні заходи захисту інформації, які виконуються на ТОВ «Нова Пошта». В процесі виконання аналізу всім технічним заходам, виконуваних, присвоюється значення «1», які не виконуються «0». Аналіз результатів технічних заходів захисту інформації ТОВ наведений у в таблиці 3.10.

Таблиця 3.10 Аналіз технічних заходів захисту інформації

Технічні заходи захисту інформації	Оцінка виконання технічних заходів захисту інформації
1	2
Реалізація дозволеної кількості допуску виконавців до інформації та документів у системі	1
Розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів обробки (передачі) і захисту інформації	1
Контроль за діями користувачів	0
Реєстрація дій користувачів інформаційної системи	1

Розв'язка ланцюгів електроживлення об'єктів захисту за допомогою захисних фільтрів, які блокують (пригнічують) інформативний сигнал	0
Використання захищених каналів зв'язку	0
Криптографічне перетворення інформації, що обробляється і передаються засобами обчислювальної техніки і зв'язку	1
Запобігання впровадження в автоматизовані системи програм-вірусів	1
Запобігання впровадження в автоматизовані системи програмних вкладок	0
Всього	5

Таким чином (таблиця 3.11), коефіцієнт уразливості технічним заходам захисту K_m = 0,5;

Таблиця 3.11 Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості технічних заходів захисту
11–12	0,01
7–10	0,25
Менше або рівне 6	0,5
Не виконуються	0,9

5) визначення чисельного значення ризику (табл. 3.12). Ризик реалізації хоча б однієї загрози з усього переліку актуальних загроз із урахуванням наявності вразливостей по відношенню до конкурентного активу визначається загальній формулі:

$$R = R_{\text{ург}} R_n C \frac{K_0 + K_t}{2} \cdot 100\ \%,$$

де R – чисельна величина ризику реалізації загроз інформаційної безпеки;

Rугр – ймовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз;

R_n – ризик невідповідності вимогам законодавства;

C − цінність активу;

K_0 – ймовірність використання організаційних вразливостей;

K_t – ймовірність використання технічних вразливостей.

На останньому етапі «Визначення допустимого рівня ризику», з таблиці 3.12 маємо значення ризику реалізації загроз інформаційній безпеці близько 5 %, це означає, що ризик реалізації загроз інформаційної безпеки є допустимим для всіх активів. Слід звернути увагу, що високий ризик реалізації загроз інформаційній безпеці, пов'язаний з персональними даними організації.

Таблиця 3.12 Ризики реалізації загроз інформаційній безпеці для активів

Назва активу	Значення ризику реалізації загроз інформаційній безпеці, %
Персональні данні	4,433
Комерційна таємниця	3,799
Електронні документи	3,483
Електронна пошта	3,166
АРМ	2,216
Бази даних	2,533
Сервер	2,849

Таким чином, в результаті оцінки маємо список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози інформаційної безпеки ТОВ.

За допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті чого одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

Даний аналіз дозволяє врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації. Маємо зручні шаблони, які можливо поступово вдосконалюватися з збільшенням кількості доступної інформації; інструмент для проведення прозорого аналізу процесів, адаптуючись до постійно-мінливих загроз, уразливості та активам.

Управління виявленими ризиками інформаційної безпеки дозволяє швидше реагувати на зміни в системі управління та контролювати ситуацію. Використання сучасних інструментів оцінки ризиків інформаційної безпеки допомагає зміцнити «слабкі місця» в системі управління компанією.

Аналіз ризиків інформаційної безпеки підприємства дозволить підтримувати дані про безпеки підприємства в актуальному стані, оперативне розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Висновок

Запропоновано методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства.

На основі математичної матричної моделі системи захисту проведено якісний аналіз системи захисту інформації ТК.

Виконано комп’ютерне моделювання ІБ за допомогою засобів Excel.

Моделювання показало, що ризик реалізації загроз інформаційної безпеки є допустимим для всіх активів ТК, але є ризик реалізації загроз інформаційній безпеці, пов'язаний з персональними даними організації.

Таким чином, в результаті оцінки маємо список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози інформаційної безпеки ТОВ. Такий підхід до аналізу ризиків ІБ підприємства дозволить підтримувати дані про безпеки підприємства в актуальному стані, оперативне

розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Контрольні запитання

10. Що потрібно визначити на першому етапі?
11. Що таке список активів організації?
12. Як може формуватися список активів організації?
13. Що таке матриця вразливостей?
14. Що таке матриця загроз?
15. Що таке матриця контролю?
16. Що таке шкала ранжування?
17. Об'ясніть, «Ризик невідповідності законодавству в області інформаційної безпеки»?
18. Об'ясніть, як розрахувати ймовірність реалізації актуальних загроз?
19. Як здійсніть оцінка цінностей компанії?
20. Як здійснити аналіз організаційних заходів захисту інформації?
21. Як обчислити ймовірність реалізації актуальних загроз?
22. Як зробити аналіз технічних заходів захисту інформації?
23. Як обчислити ризики реалізації загроз інформаційній безпеці для активів?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП

«Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.

5. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

6. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

7. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

8. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

9. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

10. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

11. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

12. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 3

Тема : Моделювання інформаційної безпеки згідно ДСТУ 27005:2019.
Мета : Розглянути питання оцінки ризиків згідно ДСТУ 27005:2019.
Кількість годин: 4 год.
Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ до ДСТУ 27005:2019
2. Види загроз (ДСТУ 27005:2019).
3. Підходи у методах оцінки ризику (цього типу).
4. регламентує стандарт ДСТУ 27005:2019?
5. Ранжування загроз за мірою ризику.
6. Оцінка значення ймовірності та можливих наслідків ризиків.
7. Порівняння *N* загроз за загальною оцінкою активів.

Література:

1. Матеріали лекції 3.
[1, с. 8 – 12, 16 - 19]
2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Хід роботи

Порядок виконання лабораторної роботи № 3:

0 Ознайомитися з короткими теоретичними відомостями.

1 Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою матричного підходу 2.

1. Заповнити даними, згідно свого варіанту та провести розрахунки у табл. 3.1 – 3.12

2 На основі отриманих результатів, надати основні рекомендації щодо оцінки ризиків та забезпечення ІБ в даній організації.

3 Оформити звіт згідно до вимог.

4 Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.
4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені матриці.
6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.

Висновки та відповіді на контрольні питання.

Стислі теоретичні відомості

Моделювання інформаційної безпеки згідно ДСТУ 27005:2022

4.1 Методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства ДСТУ 27005:2019

Стандарт **містить вказівки щ**одо управління ризиками інформаційної безпеки в організації та базується на методі ідентифікації активів, загроз і ризику вразливості, який більше не вимагається ISO/IEC 27001.

Стандарт **не містить конкретних методів** управління ризиками інформаційної безпеки. Організація сама визначає свій підхід до управління

ризиками, залежно, наприклад, від сфери застосування системи управління інформаційною безпекою (СУІБ), контексту управління ризиками або галузі промисловості.

У наступних прикладах для опису якісних оцінок використовуються значення параметрів, що обрані випадково тільки для наглядної демонстрації прикладів.

4.1 Ведення до застосування (приклад 1)

У методах оцінки ризику цього типу фактичні або запропоновані фізичні активи оцінюються з точки зору витрат на заміну або реконструкцію (тобто кількісних вимірювань). Потім ці витрати перетворюються на ту саму якісну шкалу, яка використовується для інформації (див. нижче). Фактичні чи запропоновані активи програмного забезпечення оцінюються так само, як і фізичні активи, з ідентифікацією витрат на придбання або реконструкцію, а потім конвертованими в тій самій якісній шкалі, що використовується для інформації. Крім того, якщо виявлено, що будь-яке прикладне програмне забезпечення має власні внутрішні вимоги щодо конфіденційності чи цілісності (наприклад, якщо вихідний код сам по собі є комерційно чутливим), воно оцінюється так само, як і інформація.

Цінність інформації отримується шляхом опитування керівництва підприємства («власники даних»), яке може авторитетно говорити про дані, щоб визначити цінність і конфіденційність даних, які фактично використовуються, або які будуть зберігатися, оброблятися чи мати доступ. Інтерв'ю полегшує оцінку цінності та чутливості інформації з точки зору найгірших сценаріїв, які можна обґрунтовано очікувати через несприятливі наслідки для бізнесу через несанкціоноване розкриття, несанкціоновану модифікацію, недоступність протягом різних періодів часу та знищення.

Оцінка здійснюється з використанням інструкцій з оцінки інформації, які охоплюють такі питання, як:

- особиста безпека;
- особиста інформація та конфіденційність;
- правозастосування;
- комерційно-економічні інтереси;
- фінансові втрати/зрив діяльності.

Рекомендації полегшують ідентифікацію значень у числовій шкалі, такій як шкала від 0 до 4, показана у прикладі матриці нижче, таким чином уможливлюючи розпізнавання кількісних значень, де це можливо та логічно, та якісних значень, де кількісні значення неможливі, наприклад, для загроза життю людини.

Наступним основним заходом є заповнення пар анкет для кожного типу загрози, для кожної групи активів, до яких відноситься тип загрози, щоб уможливити оцінку рівнів загроз (ймовірність виникнення) та рівнів уразливості (легкість використання). загрозою спричинення несприятливих наслідків). Кожна відповідь на запитання має бали. Ці оцінки накопичуються через базу знань і порівнюються з діапазонами. Це ідентифікує рівні загрози, скажімо, від високого до низького масштабу та рівні вразливості аналогічно, як показано в прикладі матриці нижче, розрізняючи типи наслідків залежно від того. Інформацію для заповнення анкет слід зібрати під час інтерв'ю з відповідними технічними особами, персоналом і особами, які займаються розміщенням, а також перевірки фізичного місця розташування та перегляду документації.

Значення активів, а також рівні загрози та вразливості, що стосуються кожного типу наслідків, зіставляються в матриці, як показано нижче, щоб визначити для кожної комбінації відповідну міру ризику за шкалою від 0 до 8. Значення є розміщені в матриці структурованим чином. Нижче наведено приклад (табл. 4.1).

Таблиця 4.1 Приклад 1.

	Імовірність виникнення - Загроза	Низький			Середній			Високий		
	Простота експлуатації	L	M	H	L	M	H	L	M	H
Вартість активів	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для кожного активу розглядаються відповідні вразливості та відповідні їм загрози. Якщо існує вразливість без відповідної загрози або загроза без відповідної вразливості, наразі ризику немає (але слід бути обережним, якщо ця ситуація зміниться). Тепер відповідний рядок у матриці ідентифікується за вартістю активів, а відповідний стовпець визначається за ймовірністю виникнення загрози та легкістю використання. Наприклад, якщо актив має значення 3, загроза є «високою», а вразливість «низькою», показник ризику дорівнює 5. Припустімо, що актив має значення 2, наприклад, для модифікація, рівень загрози «низький», а легкість експлуатації — «висока», тоді міра ризику дорівнює 4. Розмір матриці з точки зору кількості категорій ймовірності загрози, категорій простоти експлуатації та кількості категорій оцінки активів, можна налаштувати відповідно до потреб організації. Додаткові стовпці та рядки вимагають додаткових заходів ризику. Значення цього підхід полягає в ранжуванні ризиків, на які необхідно звернути увагу.

Подібна матриця, наведена в таблиці 4.2, є результатом розгляду ймовірності сценарію інциденту, зіставленого з оціненим впливом на бізнес. Ймовірність сценарію інциденту визначається загрозою, яка з певною ймовірністю використовує вразливість. Таблиця порівнює цю ймовірність із впливом на бізнес, пов’язаним зі сценарієм інциденту.

Отриманий ризик вимірюється за шкалою від 0 до 8, яку можна оцінити за критеріями прийнятності ризику. Ця шкала ризику також може бути зіставлена з простим загальним рейтингом ризику, наприклад, як:

— Низький ризик: від 0 до 2;

— Середній ризик: від 3 до 5;

— Високий ризик: від 6 до 8.

Таблиця 4.2 Ймовірність сценарію інциденту.

	Ймовірність з інциденту сценарію	Дуже Низький (Дуже на вряд чи)	Низький (Вряд чи)	Середина (Можливий)	Високий (Ймовірний)	Дуже Високий (Частий)
Бізнес Вплив	Дуже низький	0	1	2	3	4
	Низький	1	2	3	4	5
	Середина	2	3	4	5	6
	Високий	3	4	5	6	7
	Дуже високий	4	5	6	7	8

4.1 Ранжування загроз за мірою ризику.

Матриця або таблиця, подібна до наведеної в таблиці 4.3, може бути використана для зв’язку факторів наслідків (вартість активів) і ймовірності виникнення загрози (з урахуванням аспектів уразливості). Першим кроком є оцінка наслідків (вартості активів) за заздалегідь визначеною шкалою, напр. від 1 до 5 кожного загрозливого активу (стовпець «b» у таблиці). Другим кроком є оцінка ймовірності виникнення загрози за заздалегідь визначеною шкалою, напр. від 1 до 5 кожної загрози (колонка «c» у таблиці). Третій крок полягає в обчисленні міри ризику шляхом множення (b x c). Нарешті, загрози можна ранжувати в порядку пов’язаної з ними міри ризику.

В цьому прикладі 1 береться як найменший наслідок і найменша ймовірність виникнення.

Таблиця 4.3 Зв’язок факторів наслідків і ймовірності виникнення загрози

Загроза дескриптор	Наслідок (вартість активів)	Ймовірність загроз	міра ризику	Рейтинг загроз
(a)	(b)	(c)	(d)	(e)
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1
Загроза D	1	3	3	5
Загроза E	4	1	4	4
Загроза F	2	4	8	3

Як показано вище, це процедура, яка дозволяє порівнювати різні загрози з різними наслідками та ймовірністю виникнення та ранжувати їх у порядку пріоритету, як показано тут. У деяких випадках необхідно пов’язати грошові значення з використаними тут емпіричними шкалами.

4.2 Оцінка значення ймовірності та можливих наслідків ризиків.

У цьому прикладі наголос робиться на наслідки інцидентів інформаційної безпеки (тобто сценарії інцидентів) і на визначення того, яким системам слід надати пріоритет. Це робиться шляхом оцінки двох значень для кожного активу та ризику, які разом визначатимуть оцінку для кожного активу. Коли всі оцінки активів для системи підсумовуються, визначається міра ризику для цієї системи.

Спочатку кожному активу присвоюється вартість. Це значення стосується потенційних несприятливих наслідків, які можуть виникнути, якщо актив опиниться під загрозою. Для кожної відповідної загрози для активу це значення активу призначається активу.

Далі оцінюється значення ймовірності. Це оцінюється за поєднанням

ймовірності виникнення загрози та легкості використання вразливості, див. таблицю 4.4, де вказано ймовірність сценарію інциденту.

Таблиця 4.4 Поєднання ймовірності загрози та вразливості

Ймовірність загрози	Low			Medium			High		
Рівні вразливості	L	M	H	L	M	H	L	M	H
Цінність ймовірності сценарію інциденту	0	1	2	1	2	3	2	3	4

Далі оцінка активу/загрози призначається шляхом знаходження перетину вартості активу та значення ймовірності в таблиці 4.5. Оцінки активів/загроз підсумовуються для отримання загальної оцінки активів.

Це можна використовувати розрізняти активи, що є частиною системи.

Таблиця 4.5 Вартість активу та значення ймовірності

Вартість активу	**0**	**1**	**2**	**3**	**4**
Цінність правдоподібності					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Останнім кроком є підсумовування всіх загальних балів активів для активів системи, утворюючи бал системи. Це можна використовувати, щоб розрізняти системи та визначати, захист якої системи має бути пріоритетним.

4.5. Порівняння *N* загроз за загальною оцінкою активів

У наступних прикладах усі значення вибрано випадковим чином.

Припустимо, що система S має три активи A1, A2 і A3. Також припустимо, що існують дві загрози T1 і T2, застосовні до системи S. Нехай значення A1 дорівнює 3. Аналогічно, нехай вартість активу A2 дорівнює 2, а вартість активу A3 дорівнює 4.

Якщо для Al і T1 ймовірність загрози низька, а легкість використання вразливості середня, тоді значення ймовірності дорівнює 1 (табл. 4.6).

Таблиця 4.6 Ймовірність загрози.

Ймовірність загрози	Low			Medium			High		
Рівні вразливості	L	M	H	L	M	H	L	M	H
Цінність ймовірності сценарію інциденту	0	1	2	1	2	3	2	3	4

Оцінка активу/загрози A1/T1 може бути отримана з табл. 4.7 як перетин значення активу 3 і значення ймовірності 1, тобто 4. Подібним чином, для A1/T2 нехай імовірність загрози є середньою, а легкість використання вразливості є високою, що дає оцінку A1/T2 6.

Таблиця 4.7 Оцінка активу/загрози

			A1/T2	A1/T1	
Вартість активу	0	1	**2**	**3**	4
Ймовірність правдоподібності					
0	0	1	2	3	4
1	1	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	**6**	7	8

Тепер можна розрахувати загальну оцінку активів AIT = 4+6 =10.

Загальну оцінку активів обчислюють для кожного активу та відповідної загрози.

Загальна системна оцінка ST обчислюється додаванням:

$$ST = A1T + A2T + A3T.$$

Тепер різні системи можна порівнювати, щоб установити пріоритети та порівнювати різні активи в одній системі.

Контрольні запитання

1. Що регламентує стандарт ДСТУ 27005:2019?
2. Як визначається цінність інформації, активів?
3. Як визначається ймовірність виникнення загроз?
4. Як можна ранжувати шкалу (приклади)?
5. Як обирати шкалу?
6. Ранжування загроз за мірою ризику.
7. Формування пар вразливість- загрози.
8. Оцінка значення ймовірності та можливих наслідків ризиків.
9. Поєднання ймовірності загрози та вразливості.
10. Порівняння N загроз за загальною оцінкою активів.
11. Оцінка активу/загрози.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

2. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

13. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.
14. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)
15. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.
16. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

17. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.
18. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.
19. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.
20. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

Інформаційні ресурси в Інтернеті:

21. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).
22. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).
Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 4
Тема: Метод оцінки ризиків на основі моделі загроз і вразливостей

.

Мета роботи:

1. Поглиблення та закріплення теоретичних знання з питань:
- поняття ризиків інформаційної безпеки та їх аналіз;
- Метод оцінки ризиків на основі моделі загроз і вразливостей.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1.Ознайомлення та дослідження методу оцінки ризиків на основі моделі загроз і вразливостей

2.Набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення ІБ.

Висновки.

Література:

1. Матеріали лекції 4.

[1, с. 8 – 12, 16 - 19]

2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Хід роботи

Порядок виконання лабораторної роботи № 4:

1. Ознайомитися з короткими теоретичними відомостями.

2. Провести оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою методу оцінки ризиків на основі моделі загроз і вразливостей.
3. Заповнити даними, згідно свого варіанту та провести розрахунки у табл. 4.1 – 4.5
4. На основі отриманих результатів, надати основні рекомендації щодо оцінки ризиків та забезпечення ІБ в даній організації.
5. Оформити звіт згідно до вимог.
6. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.
4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені матриці.
6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.
7. Висновки та відповіді на контрольні питання.

Стислі теоретичні відомості

Метод оцінки ризиків на основі моделі загроз і вразливостей

Для того, щоб оцінити ризик інформації, **аналізуються всі загрози**, які діють на інформаційну систему, і уразливості, через які можлива реалізація загроз.

Виходячи з введених власником інформаційної системи даних, **будується модель загроз і вразливостей**, актуальних для інформаційної системи компанії.

На основі отриманої моделі проводиться **аналіз ймовірності реалізації загроз інформаційної безпеки на кожен ресурс** і, виходячи з цього, розраховуються ризики.

Основні поняття та припущення моделі

Базові загрози інформаційній безпеці - порушення конфіденційності, порушення цілісності та відмова в обслуговуванні.

Ресурс - будь-який контейнер, призначений для зберігання інформації, схильний до погроз інформаційної безпеки (сервер, робоча станція, переносний комп'ютер).

Властивостями ресурсу є: перелік загроз, які впливають на нього, і критичність ресурсу.

Загроза - дія, яка потенційно може привести до порушення безпеки.

Властивістю загрози є перелік вразливостей, за допомогою яких може бути реалізована загроза.

Уразливість - це слабке місце в інформаційній системі, що може привести до порушення безпеки шляхом реалізації певної загрози. Властивостями уразливості є: ймовірність (простота) реалізації загрози через дану уразливість і критичність реалізації загрози через дану уразливість.

Критичність ресурсу (D) - збиток, який понесе компанія від втрати ресурсу. Здається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи, може складатися з **критичності ресурсу по конфіденційності, цілісності та доступності (Dc, Di, Da)**.

Критичність реалізації загрози (ER) - ступінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу. Здається в процентах. Складається з **критичності реалізації загрози по конфіденційності, цілісності та доступності (ERc, ERi, ERa**).

Імовірність реалізації загрози через дану уразливість в протягом року (P (V)) - ступінь можливості реалізації загрози через дану уразливість в тих чи інших умовах. Вказується у відсотках.

Максимальна критичний час простою (Tmax) - значення часу простою, яке є критичним для організації. Тобто збиток, нанесений організації при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичне, збиток, нанесений організації, не збільшується.

Розрахунок ризиків за загрозою інформаційної безпеки

На першому етапі розраховується рівень загрози по уразливості *Th* на основі критичності і ймовірності реалізації загрози через дану уразливість.

Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

Для того, щоб оцінити ризик інформації, **аналізуються всі загрози**, які діють на інформаційну систему, і уразливості, через які можлива реалізація загроз. Виходячи з введених власником інформаційної системи даних, **будується модель загроз і вразливостей**, актуальних для інформаційної системи компанії.

На основі отриманої моделі проводиться **аналіз ймовірності реалізації загроз інформаційної безпеки на кожен ресурс** і, виходячи з цього, розраховуються ризики.

Основні поняття та припущення моделі

Базові загрози інформаційній безпеці - порушення конфіденційності, порушення цілісності та відмова в обслуговуванні.

Ресурс - будь-який контейнер, призначений для зберігання інформації, схильний до погроз інформаційної безпеки (сервер, робоча станція, переносний комп'ютер).

Властивостями ресурсу є: перелік загроз, які впливають на нього, і критичність ресурсу.

Загроза - дія, яка потенційно може привести до порушення безпеки.

Властивістю загрози є перелік вразливостей, за допомогою яких може бути реалізована загроза.

Уразливість - це слабке місце в інформаційній системі, що може привести до порушення безпеки шляхом реалізації певної загрози. Властивостями уразливості є: ймовірність (простота) реалізації загрози через дану уразливість і критичність реалізації загрози через дану уразливість.

Критичність ресурсу (D) - збиток, який понесе компанія від втрати ресурсу. Здається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи, може складатися з **критичності ресурсу по конфіденційності, цілісності та доступності (Dc, Di, Da)**.

Критичність реалізації загрози (ER) - ступінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу. Здається в процентах. Складається з **критичності реалізації загрози по конфіденційності, цілісності та доступності (ERc, ERi, ERa**).

Імовірність реалізації загрози через дану уразливість в протягом року (P (V)) - ступінь можливості реалізації загрози через дану уразливість в тих чи інших умовах. Вказується у відсотках.

Максимальна критичний час простою (Tmax) - значення часу простою, яке є критичним для організації. Тобто збиток, нанесений організації при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичне, збиток, нанесений організації, не збільшується.

Розрахунок ризиків за загрозою інформаційної безпеки

1. На першому етапі розраховується рівень загрози по уразливості Th на основі критичності і ймовірності реалізації загрози через дану уразливість.

Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} x \frac{P(V)_{c,i,a}}{100},$$

де $ER_{c,i,a}$ - критичність реалізації загрози (%);

$P(V)_{c,i,a}$ – ймовірність реалізації загрози через дану вразливість.

Обчислюється одне або три значення залежно від кількості базових загроз.

Виходить значення рівня ***загрози по уразливості*** в інтервалі від 0 до 1.

Для розрахунку рівня загрози за всіма вразливостями *CTh*, через які можлива реалізація даної загрози на ресурсі, підсумовуються отримані рівні загроз через конкретні уразливості за такою формулою:

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th),$$

Для режиму з трьома базовими загрозами:

$$CThc = 1 - \prod_{i=1}^{n}(1 - Thc),$$
$$CThi = 1 - \prod_{i=1}^{n}(1 - Thi),$$
$$CTha = 1 - \prod_{i=1}^{n}(1 - Tha),$$

Значення рівня загрози за всіма вразливістю виходять в інтервалі від 0 до 1.

3. Аналогічно розраховується загальний рівень загроз ресурсу CTh_R (враховуючи всі загрози, що діють на ресурс):

Для режиму з однією базовою загрозою:

$$CThR = 1 - \prod_{i=1}^{n}(1 - Th),$$

Для режиму з трьома базовими загрозами:

$$CThRc = 1 - \prod_{i=1}^{n}(1 - Thc),$$
$$CThRi = 1 - \prod_{i=1}^{n}(1 - Thi),$$
$$CThRa = 1 - \prod_{i=1}^{n}(1 - Tha),$$

Значення загального рівня загрози виходить в інтервалі від 0 до 1.

4. Ризик за ресурсом R розраховується так.

Для режиму з однією базовою загрозою:

$$R = CThR\ x\ D,$$

де D – критичність ресурсу. Задається в грошах чи рівнях.

У разі загрози доступність (відмова в обслуговуванні) критичність ресурсу на рік обчислюється за такою формулою:

$$D_{a/\text{рік}} = D_{a/\text{год}}\ x\ T,$$

Для інших загроз критичність ресурсу задається на рік.

Для режиму з трьома базовими загрозами:

$$Rc = CThRc\ x\ Dc,$$
$$Ri = CThRi\ x\ Di,$$
$$Ra = CThRa\ x\ Da,$$

де $D_{c,i,a}$ – критичність ресурсу за трьома загрозами. Задається в грошах чи рівнях.

Сумарний ризик за трьома загрозами:

$$R = (1 - \prod_{i=1}^{3}(1 - \frac{Ri}{100}))x100.$$

Таким чином, виходить значення ризику ресурсу в рівнях (заданих користувачем) або грошах.

5. Ризик по інформаційній системі CR

Для режиму з однією базовою загрозою:

- для режиму роботи в грошах:

$$CR = \sum_{i=1}^{n} R_i,$$

- для режиму роботи у рівнях:

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{Ri}{100}))x100.$$

Для режиму роботи з трьома загрозами:

- для режиму роботи в грошах:

$$CR_{a,c,i} = \sum_{i=1}^{n} R_i,$$
$$CR = \sum_{i=1}^{n} CR_{a,c,i},$$

$CR_{a,c,i}$ - ризик по системі по кожному виду загроз;

CR - ризик по системі по кожному виду загроз.

- для режиму роботи на рівнях:

$$CR_{a,i,c} = (1 - \prod_{i=1}^{n}(1 - \frac{Ri}{100}))x100.$$

$$CR = (1 - \prod_{i=1}^{3}(1 - \frac{R_{a,i,c}}{100}))x100.$$

Завдання контрзаходів

Для розрахунку ефективності введеного контрзаходу необхідно пройти послідовно по всьому алгоритму з урахуванням заданого контрзаходу. Тобто, на виході користувач отримує значення двох ризиків – ризику без урахування контрзаходу *Rold* та ризик з урахуванням заданого контрзаходу *Rnew* (або з урахуванням того, що вразливість закрита).

Ефективність введення контрзаходу *E* розраховується за формулою:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результаті роботи алгоритму користувач системи отримує такі дані:

• Ризик за трьома базовими загрозами (або однією сумарною загрозою) для ресурсу;

• Ризик сумарно за всіма загрозами ресурсу;
• Ризик за трьома базовими загрозами (або однією сумарною загрозою) для інформаційної системи;
• Ризик усіх загроз для інформаційної системи;
• Ризик усіх загроз для інформаційної системи після завдання контрзаходів;
• Ефективність контрзаходу;
• Ефективність комплексу контрзаходів.

Приклад розрахунку ризику інформаційної безпеки на основі моделі загроз та вразливостей

Таблиця 4.1

Ресурс	Загрози	Вразливість
Сервер (критичность ресурса 100 у.е.)	**Загроза 1** Неавторизоване проникнення порушника всередину периметра, що охороняється (одного з периметрів)	**Вразливість 1** Відсутність регламенту доступу до приміщень з ресурсами, що містять цінну інформацію
		Вразливість 2 Відсутність системи спостереження (відеоспостереження, сенсори тощо) за об'єктом (або існуюча система спостереження охоплює не всі важливі об'єкти)
	Загроза 2 Неавторизована модифікація інформації в системі електронної пошти, що зберігається на ресурсі	**Вразливість 1** Відсутність авторизації для внесення змін до системи електронної пошти
		Вразливість 2 Відсутність регламенту роботи із системою криптографічного захисту електронної кореспонденції
	Загроза 3 Розголошення конфіденційної інформації співробітниками компанії	**Вразливість 1** Відсутність угод про конфіденційність
		Вразливість 2 Розподіл атрибутів безпеки (ключ доступу, шифрування) між кількома довіреними співробітниками

Таблиця 4.2 Вхідні данні

Ресурси АС	**Загроза/Вразливість**	**Ймовірність реалізації через дану вразливість за рік (%), *P*(*V*)**	**Критичність реалізації загрози через вразливість (%), *ER***
1	Загроза1/Вразливість1	50	60
	Загроза1/Вразливіст2	20	60
	Загроза2/Вразливість1	60	40
	Загроза2/Вразливіст2	10	40
	Загроза3/Вразливість1	10	80
	Загроза3/Вразливіст2	80	80
2	Загроза1/Вразливість1	10	60

	Загроза1/Вразливість2	20	60
	Загроза2/Вразливість1	20	40
	Загроза2/Вразливість2	60	40
	Загроза3/Вразливість1	10	80
	Загроза3/Вразливість2	80	80

Таблиця 4.3 Рівень по загрозам

Ресурси АС	**Загроза/Вразливість**	**Рівень загрози (%), *Th***	**Рівень загрози за всіма вразливастями, що реалізують дану загрозу (%), *CTh***
1	Загроза1/Вразливість1	0,30	0,38
	Загроза1/Вразливість2	0,12	
	Загроза2/Вразливість1	0,24	0,27
	Загроза2/Вразливість2	0,04	
	Загроза3/Вразливість1	0,08	0,67
	Загроза3/Вразливість2	0,64	
2	Загроза1/Вразливість1	0,06	0,17
	Загроза1/Вразливість2	0,12	
	Загроза2/Вразливість1	0,08	0,30
	Загроза2/Вразливість2	0,24	
	Загроза3/Вразливість1	0,08	0,67
	Загроза3/Вразливість2	0,64	

Таблиця 4.4 Рівень по ресурсам

Ресурси АС	**Загроза/Вразливість**	**Рівень загрози за всіма вразливастями, що реалізують дану загрозу (%), *CTh***	**Загальний рівень загроз по ресурсу (%), *CThR***
1	Загроза1/Вразливість1	0,38	0,85
	Загроза1/Вразливість2		
	Загроза2/Вразливість1	0,27	
	Загроза2/Вразливість2		
	Загроза3/Вразливість1	0,67	
	Загроза3/Вразливість2		
2	Загроза1/Вразливість1	0,17	0,81
	Загроза1/Вразливість2		

	Загроза2/Вразливість1	0,30	
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1	0,67	
	Загроза3/Вразливіст2		

Таблиця 4.5 Ризик по ресурсам

Ресурси АС	**Загроза/Вразливість**	**Загальний рівень загроз по ресурсу (%), *CThR***	**Ризик ресурсу (у.о), *R***
1	Загроза1/Вразливість1	0,851	85,11
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1		
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1		
	Загроза3/Вразливіст2		
2	Загроза1/Вразливість1	0,808	80,84
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1		
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1		
	Загроза3/Вразливіст2		

1. На основі отриманих даних зробити загальні висновки з виконаної роботи, а також визначити основні напрями удосконалення СЗІ об’єкта.

Завдання

1. До заданих інформаційних ресурсів та інформаційних потоків (визначених у попередній роботі) визначити перелік загроз (не менше 20).

2. Знайти у загальнодоступних джерелах статистику частоти появи цих загроз.

3. Визначити відповідно до знайденої статистики ймовірність виникнення, кожної загрози.

4. Зробити висновки, щодо адекватності знайденої статистики об’єкту захисту.

Контрольні запитання

1. Що потрібно визначити на першому етапі?
2. Що таке список активів організації?
3. Як може формуватися список активів організації?

4. Що таке матриця вразливостей?
5. Що таке матриця загроз?
6. Що таке матриця контролю?
7. Що таке шкала ранжування?
8. Об’ясніть, «Ризик невідповідності законодавству в області інформаційної безпеки»?
9. Об’ясніть, як розрахувати ймовірність реалізації актуальних загроз?
10. Як здійсніть оцінка цінностей компанії?
11. Як здійснити аналіз організаційних заходів захисту інформації?
12. Як обчислити ймовірність реалізації актуальних загроз?
13. Як зробити аналіз технічних заходів захисту інформації?
14. Як обчислити ризики реалізації загроз інформаційній безпеці для активів?

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.

5. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник

наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

6. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

7. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

8. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

9. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

10. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

11. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

12. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

13. Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 5

Тема: Розв’язання завдань прийняття рішень з векторними критеріями

Мета роботи: Набуття досвіду та закріплення знань та отримання практичних навичок вирішення задач прийняття рішень з векторними критеріями.

Кількість годин: 4 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Рішення задач з векторними критеріями.
2. Правило абсолютної переваги.
3. Перевага по правилу більшості
4. Виділення кращих об'єктів за допомогою таблиці бальних оцінок.
5. Зведення векторного критерію до скалярного.
6. Зведення багатокритеріальної задачі для пошуку екстремуму єдиної цілі в умовах обмежених
7. Лексикографічний метод вирішення багатокритеріальних задач.

Література:

1. Матеріали лекції 5.

[1, с. 8 – 12, 16 - 19]

2. Нормативні документи [1 - 10].

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Теоретичні відомості

2.1. Рішення задач з векторними критеріями

Допустимо задано безліч об'єктів $X = \{x_1, ..., x_n\}$, кожен з яких оцінюється векторним критерієм з m компонентами $K = (k_1, ..., k_m)$. Потрібно за допомогою критерію K із безлічі об'єктів X виділити найкращий об'єкт.

Для вирішення сформульованої задачі кожен із об’єктів сукупності $X = \{x_1,..., x_n\}$ оцінюється за допомогою компонента $k_1, ..., k_m$ вартісного критерію, а результати цієї оцінки показано в табл. 1. Будемо розглядати після цього об’єкти $x_1, ..., x_n$ просто як набори відповідних їм числових значень показників $(k_1(x_1), ..., k_m(x_1)), ..., (k_1(x_n), ..., k_m(x_n))$, що включають у себе всю інформацію про основні об’єкти. В результаті такого переходу порівняння вихідних об’єктів за критерієм K зводиться до порівняння рядка табл. 1.

Таблиця 1

	k_1	...	k_j	...	k_m
x_1	$k_1(x_1)$	...	$k_j(x_1)$	...	$k_m(x_1)$
. . .	. . .	... ...	. . .	... ...	. . .
x_i	$k_1(x_i)$	...	$k_j(x_i)$	...	$k_m(x_i)$
. . .	. . .	... ...	. . .	... ...	. . .
x_n	$k_1(x_n)$	...	$k_j(x_n)$	...	$k_m(x_n)$

Для виділення кращого об'єкта з допомогою табл. 1 необхідний набір правил, який дозволяє порівняти пару будь-яких об’єктів $x_k, x_l \in X$ і встановити, є чи один з об’єктів кращим іншим або ні. Такий набір правил називається системою вирішальних правил. Розглянемо кілька типів, найбільш часто застосовуваних вирішальних правил. Однак спочатку для посилення наслідків викладення (но без втрати спільноти) положим, що використовується такий векторний критерій $K = (k_1, ..., k_m)$, що значення будь-якого компонента k_j $(j = \overline{1, m})$ у відношенні кожного об’єкта x_i краще (краще), ніж воно більше.

2.1.1. Правило абсолютної переваги

Об'єкт x_k вважається кращим об'єктом x_l тоді і тільки тоді, коли для всіх компонентів ринку критерії $K = \{k_1, \ ..., \ k_m\}$ виконуються співвідношення

$$k_j(x_k) \geq k_j(x_l), \ j = \overline{1, m}. \qquad (1)$$

Таким чином, це вирішальне правило припускає, що найкращий об'єкт не є вищим за інший об'єкт ні за одним компонентом критерію виробництва.

Приклад 1. Потрібно з чотирьох місць роботи A, B, C, D вибрати краще. При цьому кожне місце роботи оцінюється за чотирма показниками k_1, k_2, k_3, k_4: розмір зарплати, тривалість відпуску, час поїздки на роботу і перспектива майбутнього зростання співробітника (табл. 2).

Таблиця 2

	Розмір зарплати, грн.	Тривалість відпустки, дні	Час поїздки на роботу, хв.	Перспектива зростання
А	1800 рік	30	20	Повільне зростання
Б	1400	30	30	Повільне зростання
С	1200	48	40	Швидкий ріст
Д	2400	24	10	Відсутність зростання

Безпосередньо вирішити цю задачу, використовуючи правило абсолютної переваги, оскільки для оцінки місця роботи використовується один якісний показник (перспектива зростання) і один показник (час поїздки на роботу), який не відповідає прогнозу щодо того, що, чим його значення більше, тим альтернатива краще. У зв'язку з цим необхідно сформувати вихідну задачу. Для цього замість показника k_3 (час поїздки на роботу) введемо показник економії часу в порівнянні з часом самої тривалої поїздки на роботу:

$$k_3^* = 40 - k_3.$$

Замість якісного показника k_4 введем кількісний показник k_4^* за допомогою табл. 3.

З вектором показників $(k_1, \ k_2, \ k_3^*, \ k_4^*)$ табл. 2 перетворюється до нового вигляду (табл. 4).

Таблиця 3

k_4	k_4^*
Відсутність перспективи службового зростання працівника у майбутньому	0

Повільне службове зростання співробітника у майбутньому	1
Середня швидкість службового зростання співробітника у майбутньому	2
Швидке зростання за службовим становищем співробітника в майбутньому	3

Таблиця 4

	k_1	k_2	k_3^*	k_4^*
А	1800 рік	30	20	1
Б	1400	30	10	1
С	1200	48	0	2
Д	2400	24	30	0

У відношенні альтернативних таблиць 4 співвідношення (1) виконуються тільки для єдиної пари місць роботи A і B : місце роботи A бажане місце роботи B за показниками k_1 і k_3^* і однаково за показниками k_2 і k_4^*. Для інших пар альтернатив (місце праці) установити перевагу за допомогою правил абсолютної переваги не вдається. Подібна ситуація спостерігається і при вирішенні інших завдань з векторним критерієм за допомогою цих правил.

Основний недолік правил абсолютного переваги полягає в вузький області його застосовності, іншими словами, воно є "слабим", як застосовне для вирішення відносно невеликого числа практичних завдань.

Важливою перевагою правила абсолютної переваги є його транзитивність, тобто є, якщо альтернатива A краща альтернатива B ($A > B$), яка, у свою чергу, краща альтернатива C ($B > C$), до альтернативи A краща альтернатива C ($A > C$) .

2.1.2. Перевага по правилу більшості

Для отримання більш сильного правила, ніж правило абсолютного переваги, положим, що альтернатива x_k бажані альтернативи x_l, якщо співвідношення (1) виконуються не для всіх показників, а тільки для більшості. Якщо альтернатива x_k по частині показників краще альтернативи x_l і за таким же числом показників уступає ей, то альтернативи x_k і x_l вважаються еквівалентними ($x_k \approx x_l$) або нерізними (однаковими). Застосував це правило к табл. 4, отримаю:

$$A > B \, , A \approx C \, , A \approx D \, , B \approx C \, , B \approx D \, , C \approx D \, .$$

Таким чином, за правилом більшість усіх альтернатив порівняні між собою. Однак вибрати кращу альтернативу в розглянутому прикладі за допомогою цього правила не дається, оскільки порушується відношення транзитивності: $A \approx S$, $S \approx V$, але $A > B$.

Таке порушення транзитивності при визначенні переваги за правилом більшості іноді називають парадоксом голосування при застосуванні більшості правил.

2.1.3. Виділення кращих об'єктів за допомогою таблиці бальних оцінок

Якщо у третьому стовбець табл. 4 число 20 заміряти на 2, 10 на 1 і 30 на 3, формально за показником k_3^* при використанні співвідношення (1) залишається попереднім перевага між аналізованими альтернативами, а фактично, для людини, що вибирає місце роботи, ситуація змінилася, оскільки за третім показником все альтернативи стали однаковими. У зв'язку з цим числове задання показників не завжди зручно. Часто краще використовувати не конкретні числові значення в визначених одиницях, а також деякі більш загальні оцінки, які можна задати в абстрактних одиницях або балах. При цьому для кожного показника встановлюється визначене число рівнів відмінностей або градацій. У якості низького балу задають 0 або 1, а при переході до наступного рівня значення показника збільшується на один бал.

Табл. 1, значення показників, в яких виражені в балах, називають таблицею бальних оцінок.

Розглянемо приклад використання таблиці бальних оцінок для виділення кращої альтернативи.

Приклад 2. Потрібне зображення бажаного покупця ПЭВМ серед моделей машин, позначених буквами: A, B, C, D, E, F, G. Оцінки цих моделей наведені в табл. 5 за наступними шістьма показниками:

k_1 – ціна (сім градації);

k_2 – тактова частота (чотири градації);

k_3 – об’єм оперативної пам’яті (п’ять градацій);

k_4 – об’єм пам’яті вінчестера (п’ять градацій);

k_5 – зовнішнє оформлення (чотири градації);

k_6 – надійність (чотири градації).

Таблиця 5

	k_1	k_2	k_3	k_4	k_5	k_6
А	6	4	4	2	2	3
Б	5	3	5	4	1	2
С	4	2	4	3	3	1
Д	6	4	5	5	2	3
Е	2	2	3	4	4	2
Ф	7	1	2	2	1	2
Г	6	4	3	3	4	4

Введемо наступне вирішальне правило: альтернатива X краще альтернативи Y, якщо число показників, за якими альтернатива X перевершує альтернативу Y, більше числа показників, за якими вона уступає альтернативу Y.

При цьому вирішальному правилі співвідношення переваг між альтернативами табл. 5 визначається табл. 6.

Таблиця 6

	А	*Б*	*С*	*Д*	*Е*	*Ф*	*Г*
А	0	1	1	0	1	1	0
Б	0	0	1	0	1	1	0
С	0	0	0	0	0	1	0
Д	1	1	1	0	1	1	0
Е	0	0	1	0	0	1	0
Ф	0	0	0	0	0	0	0
Г	1	1	1	0	1	1	0

В табл. 6 одиниця на перетині i -й рядка і j - го стовбця вказує на домінування i -й альтернативи над j -й. Якщо на перетині i -й строки і j -го стовбця і j -й строки і i -го стовбця нулі, то альтернативи знайдені.

аналіз даних табл. 6 показує, що альтернативи D і G краще всіх інших. За даним вирішальним правилом вони рівнозначні, так як альтернатива D перевершує альтернативу G за двома показниками (k_1 і k_2) і уступає її також за двома показниками (k_5 и k_6), а за показниками k_1 та k_2 інші альтернативи мають одинакові значення.

2.1.4. Зведення векторного критерію до скалярного

Допустимо в табл. 1 альтернативи оцінюються за m кількісними показниками k_j ($j = \overline{1, m}$), однак значущість кожного з показників характеризується ваговим коефіцієнтом a_j, а кожна альтернатива x_i ($i = \overline{1, n}$) характеризується зваженою сумою

$$K(x_i) = \sum_{j=1}^{m} a_j k_j(x_i).$$

Вирішальне правило в цьому випадку може бути введено таким чином: альтернатива x_k краще альтернативи x_l, якщо $K(x_k) > K(x_l)$.

Це вирішальне правило є абсолютно сильним, оскільки воно призводить до числової оцінки кожної альтернативи і, відповідно, до співвідношення порядку ≥ між альтернативами.

Недолік цього вирішального правила складається в тому, що з його допомогою векторний критерій перетворюється в скалярний, хоча компоненти вікового критерію можуть якісно відрізнятися від іншого. Тем не менше, цей критерій широко застосовується в техніці.

2.1.5. Зведення багатокритеріальної задачі для пошуку екстремуму єдиної цілі в умовах обмежених

Це досить раціональний і поширений метод вирішення задач з векторним критерієм. Частіше всього він застосовується таким чином. В результаті оптимізують одну з цілей, розглядаючи інші цілі в якості обмежених. У результаті такої послідовної оптимізації при m компонентах критеріїв виробництва може бути отримано безліч із m рішень, вибір кращого з яких у загальному випадку не є тривіальною задачею. Крім того, при вирішенні кожної оптимізаційної задачі обмеження в загальному випадку звужують область пошуку оптимуму в більшій або меншій мірі довільно. Це часто призводить до ситуації, коли дійсно оптимальне рішення знайти не удається.

Приклад 3. Розв'яжемо задачу з прикладу 2 розглянутим методом. Оскільки в цій задачі використовується векторний критерій із шістьма компонентами, то застосування методу, що зводить багатокритеріальну задачу до пошуку екстремумів за окремими критеріями в умовах обмеженості, призводить до послідовного вирішення шести оптимізованих задач. При рішенні першої з шести задач шукають альтернативи, оптимальні за першою складовою k_1 критерію оцінки. По іншим п'яти компонентам критеріїв законодавства задаються обмеження. Припустимо вони будуть наступні: по компонентам k_3 і k_4 вибраним альтернативам не потрібно приймати двох найменших значень (1 і 2), а по компонентам k_2, k_5, k_6 – найменших значень, т.е. повинні виконувати умови

$$k_j(\cdot) > 1, \quad j = 2, 5, 6;$$
$$k_j(\cdot) > 2, \quad j = 3, 4. \tag{2}$$

Якщо б не був обмежений, то кращим за першим критерієм була б альтернатива F , однак із-за порушення обмеження (2) вона обрана бути не може. Порівняння даних табл. 5 і обмеження (2) дозволяє встановити, що обмеження задовольняють тільки альтернативи D , E і G . Якщо $k_1(D) = k_1(G) = 6$ і $k_1(E) = 2$, то кращими і рівноцінними за критерієм k_1 є альтернативи D і G .

При пошуку оптимальних альтернатив за критерієм k_2 будемо полагати, що обмеження за критеріями $k_3 - k_6$ залишаються такими ж, як і при вирішенні першої задачі, а обмеження за першим критерієм задається співвідношенням.

$$k_1(\cdot) > 4. \tag{3}$$

Порівняння даних табл. 5 з обмеженнями на значення інших компонентів критерію виробництва, виділяємо альтернативи D і G , що задовольняють обмеженням (2) і (3). Якщо $k_2(D) = k_2(G) = 4$, то дві альтернативи є кращими за критерієм k_2 .

Використавши обмеження (2), (3), легко визначити оптимальні альтернативи за компонентами критеріїв виробництва $k_3 - k_6$. В результаті отримуємо наступне безліч оптимальних альтернатив для кожної з шести однокритеріальних задач:

задача 1 (з оптимізацією за критерієм k_1) { D , G };

задача 2 (з оптимізацією за критерієм k_2) { D , G };

задача 3 (з оптимізацією за критерієм k_3) { D };

задача 4 (з оптимізацією за критерієм k_4) { D };

задача 5 (з оптимізацією за критерієм k_5) { G };

задача 6 (з оптимізацією за критерієм k_6) { G }.

Таким чином, в результаті вирішення шести однокритеріальних задач не вдалося знайти рішення, оптимального по всім компонентам критеріїв виробництва. Однак число альтернатив, що претендують на оптимальне рішення вихідної задачі, зменшилося до двох.

2.1.6 Лексикографічний метод вирішення багатокритеріальних задач

Метод застосовується до задач, в яких окремі цілі мають різну вагу і їх можливо розмістити в визначеному ієрархічному порядку. У таких завданнях на першому етапі оптимізації визначають безліч рішень, які оптимізують ціль найвищого рангу. Отримане безліч D рішень на другому етапі звужуєтеся при оптимізації другої по важливості цілі. Цей процес продовжується до тих пор, поки не буде одного єдиного рішення. Якщо при оптимізації цілого найнижчого рангу не вдається знайти єдине рішення, то з безлічі залишилися рішень роблять суб'єктивний вибір, або вводять додатковий критерій. Цей метод застосовується досить широко, але передбачає ієрархію цілей.

Приклад 4. Вирішіть задачу з прикладу 2 розглянутим методом у пропозиції, що необхідно купити комп'ютер з високою швидкістю дії (ціль найвищого рангу), бажано недорогою (ціль другого рангу), але надійним (ціль третього рангу) і з великим об'ємом оперативної пам'яті (ціль четвертого рангу). ранга). Не змішало б мати достатньо великий обсяг вінчестера (ціль п'ятого рангу) і хороше зовнішнє оформлення (ціль низького рангу).

Із заданої ієрархії цілей слід, що для визначення кращого рішення необхідно послідовно використовувати компоненти критеріїв виробництва k_2, k_1, k_6, k_3, k_4 і k_5. Таким чином, для визначення кращої альтернативи необхідно послідовно вирішити шість одно-критеріальних оптимізованих завдань.

При рішенні першої з шести задач шукають оптимізовані альтернативи, оптимальні за компонентом k_2 критерію економіки. Застосування критерію k_2 к даним табл. 5 дозволяє встановити, що кращими і рівноцінними є три альтернативи: A, D, G, –оскільки $k_2(A) = = k_2(D) = k_2(G) = 4$. Отже, при вирішенні наступної оптимізованої задачі будуть оцінюватися тільки ці три альтернативи.

Рішення другого з шести оптимізованих завдань не зменшує число кращих альтернатив, оскільки $k_1(A) = k_1(D) = k_1(G) = 6$, то є альтернативи A, D, G рівноцінні и по критерію k_1.

При рішенні третьої з шести оптимізованих задач серед альтернативи A, D, G шукаються альтернативи, оптимальні за компонентом k_6 критерію витрат. Застосування критерію k_6 к даним табл. 5 дозволяє встановити, що кращим і єдиним є альтернатива G, оскільки $k_6(A) = k_6(D) = 3$, а $k_6(G) = 4$. Таким чином, застосування лексикографічного методу вирішення багатокритеріальної задачі в цьому випадку дозволяє виділити єдине краще рішення.

Підведем підсумки розгляду методів рішення задач з векторним критерієм.

Для вирішення завдань з векторним критерієм необхідно завдання деякого вирішального правила. Єдиного універсального вирішального правила не існує, однак існує безліч конкретних вирішальних правил. Вибір того чи іншого вирішального правила залежить від змістовної постановки вирішуваної задачі та суб’єктивних переваг особи, що приймає рішення. Формалізованих

загальновизнаних процедур вибору вирішальних правил в даний час не існує. Розробка таких процедур являє собою складну концептуальну проблему.

Індивідуальні завдання

1. Формалізуйте ситуацію вибору у вигляді задачі прийняття рішення з векторним критерієм при розмірах матриці не менше ніж 8 ×6.
2. Розв’язати сформульовану задачу всіма описаними в методичних вказівках методами.
3. Оформіть звіт по лабораторній роботі.

Контрольні питання

1. Рішення задач з векторними критеріями.
2. Правило абсолютної переваги.
3. Перевага по правилу більшості
4. Виділення кращих об'єктів за допомогою таблиці бальних оцінок.
5. Зведення векторного критерію до скалярного.
6. Зведення багатокритеріальної задачі для пошуку екстремуму єдиної цілі в умовах обмежених
7. Лексикографічний метод вирішення багатокритеріальних задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

1. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.
2. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

3. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.

4. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

5. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

6. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

7. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

8. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

Інформаційні ресурси в Інтернеті:

9. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

10. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

11. Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 6

Тема : Формування та дослідження моделі ІБ за ефективністю прийнятих рішень

Мета : Розглянути питання оцінки дій загроз в інформаційних системах

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1. Основні складові моделі СЗІ
2. Поняття «Основи», «Напрямки», «Етапи».
3. Принцип об'єднання матриці, та позначення.
4. **Приклад оцінки якості СЗІ**
5. Графічне зображення результатів.
6. Оцінка захищеності об'єктів ІБ.
7. Проведення оцінки вразливості та ризиків.
8. Узагальнені показники рівня захищеності ІБ.

Висновки.

Література:

1. Матеріали лекції 6.

[3, с. 8 – 12, 16 - 19]

2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Теоретичні відомості

Розглянемо три "координати вимірів" - три групи складових моделі СЗІ:
- З чого складається (“основи”).
- Для чого призначена (“напрямки”)
- Як працює (“етапи”).

Основами або складовими частинами практично будь-якої складної системи (у тому числі системи захисту інформації) є:

1) Законодавча, нормативно-правова та наукова база;

2) Структура та завдання органів (підрозділів), що забезпечують безпеку ІТ;

3) Організаційно-технічні та режимні заходи та методи (політика інформаційної безпеки);

4) Програмно-технічні способи та засоби.

Напрями формуються з конкретних особливостей ІБ як об'єкта захисту.

У загальному випадку, враховуючи типову структуру ІБ та історично сформовані види робіт із захисту інформації, пропонується розглянути наступні напрямки:

1) Захист об'єктів інформаційних систем;

2) Захист процесів, процедур та програм обробки інформації;

3) Захист каналів зв'язку;

4) Пригнічення побічних електромагнітних випромінювань.

5) Управління системою захисту;

Оскільки кожен із цих напрямів базується на перерахованих вище основах, то елементи основ і напрямів розглядаються нерозривно один з одним. Наприклад, одну з основ під назвою “Законодавча база” необхідно розглядати у всіх напрямках, а саме:

1) Законодавча база захисту об'єктів;

2) Законодавча база захисту процесів, процедур та програм;

3) Законодавча база захисту каналів зв'язку;

4) Законодавча база придушення побічних електромагнітних випромінювань;

5) Законодавча база з управління та контролю самої системи захисту.

Аналогічно слід розглядати інші межі “основ” (структуру, заходи, кошти) у всіх напрямах.

Для формування найзагальнішого уявлення про конкретну систему захисту необхідно відповісти мінімально на 20 (4 * 5 = 20) найпростіших питань. Далі необхідно розглянути "етапи" (послідовність кроків) створення СЗІ, які необхідно реалізувати однаково для кожного окремо "напрямки" з урахуванням зазначених вище "основ".

Проведений аналіз існуючих методик та послідовностей робіт зі створення СЗІ дозволяє виділити такі “етапи”:

1) Визначення інформаційних та технічних ресурсів, а також об'єктів ІВ, що підлягають захисту;

2) Виявлення повної множини потенційно можливих загроз та каналів витоку інформації;

3) Проведення оцінки вразливості та ризиків інформації (ресурсів ІВ) за наявної множини загроз та каналів витоку;

4) визначення вимог до системи захисту інформації;

5) Здійснення вибору засобів захисту інформації та їх характеристик;

6) Впровадження та організація використання обраних заходів, способів та засобів захисту.

7) Здійснення контролю цілісності та управління системою захисту.

Оскільки "етапів" сім, і по кожному треба висвітлити 20 вже відомих питань, то загалом для формування уявлення про конкретну систему захисту необхідно відповісти на 140 питань. Щодо кожного питання (елементу) виникне кілька десятків уточнень. У загальному випадку кількість елементів матриці може бути визначена із співвідношення

K = Oi * Hj * Mk, де:

- K – кількість елементів матриці
- Oi - кількість складових блоку "основи"
- Hj - кількість складових блоку "напряму"
- Mk - кількість складових блоку "етапи"

У нашому випадку загальна кількість елементів "матриці" дорівнює 140 K = 4 * 5 * 7 = 140, оскільки Oi = 4, Hj = 5, Mk = 7.

Далі для простоти розуміння спробуємо перетворити тривимірну фігуру на двовимірну. Для цього розгорнемо тривимірний куб на площині та отримаємо тривимірну матрицю у вигляді двомірної таблиці, яка допоможе логічно об'єднати складові блоків "основи", "напрямки" та "етапи" за принципом кожен з кожним.

Слід пам'ятати, що матриця у вигляді двомірної таблиці з'являється не сама по собі, а формується в кожному конкретному випадку, виходячи з конкретних завдань створення конкретної СЗІ для конкретної ІС.

2.4 Подання елементів матриці

Елементи матриці мають відповідну нумерацію. Слід звернути увагу на позначення кожного з елементів матриці, де:

1) перше знайоме місце (X00) відповідає номерам складових блоку "етапи",

2) друге знайоме місце (0X0) відповідає номерам складових блоку "напряму",

3) третє знайоме місце (00X) відповідає номерам складових блоку "основи".

(дивись файл 1.exls аркуш 2.7)

Рисунок 2.7 – нумерація та позначення кожного елемента матриці

Рисунок 2.8 - Приклад нумерації елемента матриці №321

На малюнку та 2.8 представлений приклад елемента матриці 321, який формується з урахуванням таких складових:

1) 300 - Проведення оцінки вразливості та ризиків (складова № 3 блоку "етапи");

2) 020 - Захист процесів та програм (що становить № 2 блоку "напрямки");

3) 001 - Нормативна база (складова № 1 блоку "основи");

Далі наведемо приклад змісту інформації для елементів матриці № 321, 322, 323, 324, які поєднують такі складові:

1) № 3 (300 проведення оцінки вразливості та ризиків) блоку "етапи",

2) № 2 (020 захист процесів та програм) блоку "напрямки" ,

3) № 1, 2, 3, 4 (001 нормативна база, 002 структура органів, 003 заходи, 004 використовувані засоби) блоку "основи".

Результат:

Елемент № 321 містить інформацію про те, наскільки повно відображені у законодавчих, нормативних та методичних документах питання, що визначають порядок проведення оцінки вразливості та ризиків для інформації, що використовується в процесах та програмах конкретної ІС?

Елемент № 322 містить інформацію про те, чи є структура органів (співробітники), відповідальна за проведення оцінки вразливості та ризиків для процесів та програм ІВ?

Елемент № 323 містить інформацію про те, чи визначено режимні заходи, що забезпечують своєчасне та якісне проведення оцінки вразливості та ризиків для інформації, що використовується у процесах та програмах ІС?

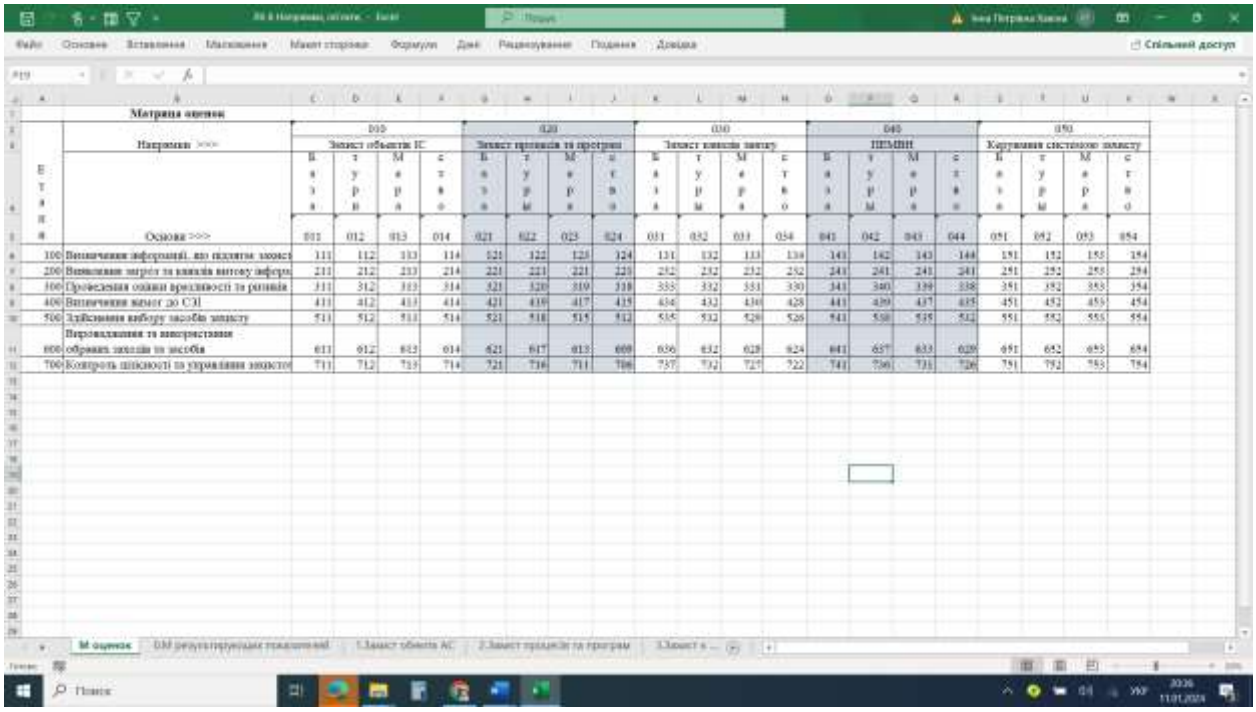
Елемент № 324 містить інформацію про те, чи застосовуються технічні, програмні чи інші засоби, для забезпечення оперативності та якості проведення оцінки вразливості та ризиків у процесах та програмах ІС?

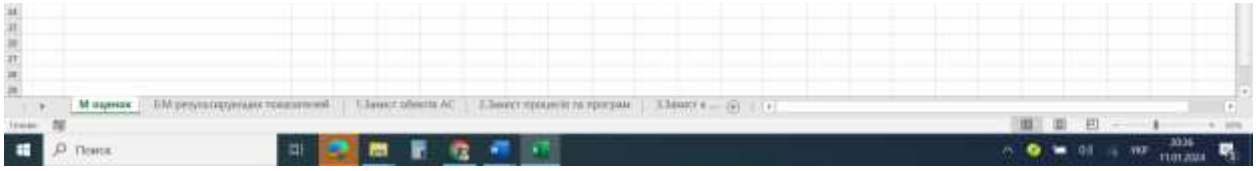
Це зміст лише чотирьох питань із ста сорока, але відповіді на них вже дозволяють сформувати певне уявлення про стан справ щодо захисту інформації в конкретній ІС.

У випадку розглядаються все 140 питань (за кількістю елементів матриці). Повний зміст 140 елементів матриці можна переглянути у файлі.

Опис набору засобів для забезпечення якості контролю цілісності та управління комплексною системою захисту інформації дозволяють скласти повне уявлення про СЗІ та оцінити досягнутий рівень захисту.

Такий підхід дає можливість тримати правильний напрямок у процесі створення складних систем захисту. При цьому постійно враховуються взаємні логічні зв'язки між численними елементами СЗІ, тобто шанси побудувати саме систему, а не набір рішень. Матриця не існує сама по собі, а формується виходячи з опису конкретної ІВ та конкретних завдань щодо захисту інформації в цій системі.





Далі формуються дані для оцінки захищеності об'єктів ІВ (перший напрямок захисту).

Зміст звіту

1. Тема лабораторної роботи.
2. Мета лабораторної роботи.
3. Індивідуальне завдання.
4. Результати виконання пунктів індивідуального завдання.
5 . Висновки щодо лабораторної роботи.

Контрольні запитання

9. Які основні складові моделі СЗІ?
10. Що входить у поняття «Основи»?
11. Що входить у поняття «Напрямки»?
12. Що входить у поняття «Етапи»?
13. Який принцип об’єднання матриці?
14. Як нумеруються елементи матриці?
15. Як позначено складові блоку «Основи»?
16. Як позначено складові блоку «Напрямки»?
17. Як позначено складові блоку «Етапи»?

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

1. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.
2. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)
3. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.
4. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

5. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.
6. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.
7. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.
8. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

Інформаційні ресурси в Інтернеті:

9. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).
10. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).
11. Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 7

Тема: Моделювання нечіткої експертної системи засобами інструментарію нечіткої логіки.

Мета: Вивчення методів побудови нечітких множин із використанням різних типів функцій власності. Ознайомиться з найпоширенішими логічними операціями над нечіткими множинами.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1.

2. Відомість проектної документації до техноробочого проекту КСЗІ в АСВТЗІ.

3. Відомість експлуатаційної документації до техноробочого проекту КСЗІ в АСВТЗІ.

4. Основні технічні рішення та заходи при створенні КСЗІ в АСВТЗІ.

4. Висновки.

Література:

1. Матеріали лекції 7.
[1, с. 8 – 12, 16 - 19]
[1, 2 ч., с. 5 - 9]
2. Нормативні документи [1 - 10].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Короткі відомості з теорії

Функції приладдя . Інструментарій нечіткої логіки (ІНЛ) у складі пакету *Matlab* містить 11 вбудованих типів функцій приналежності (ФП), що формуються на основі шматково-лінійних функцій, розподілу Гауса, сигмоїдної кривої, квадратичних та кубічних поліноміальних кривих. До найпростіших ФП можна віднести трикутну та трапецієподібну. Найменування трикутної ФП – ***trimf*** *(**Tri** angle **m** embership **f** unction).* У параметричному вигляді вона є не що інше, як набір трьох точок, що утворюють трикутник.

Опис функції:

$$y = trimf\,(x, [a\ b\ c]),$$

де вектор x – базове безліч, у якому визначається ФП. Величини a і c задають основу трикутника, b - Його вершину.

В аналітичному вигляді трикутна ФП може бути задана таким чином (рис. П1 *а):*

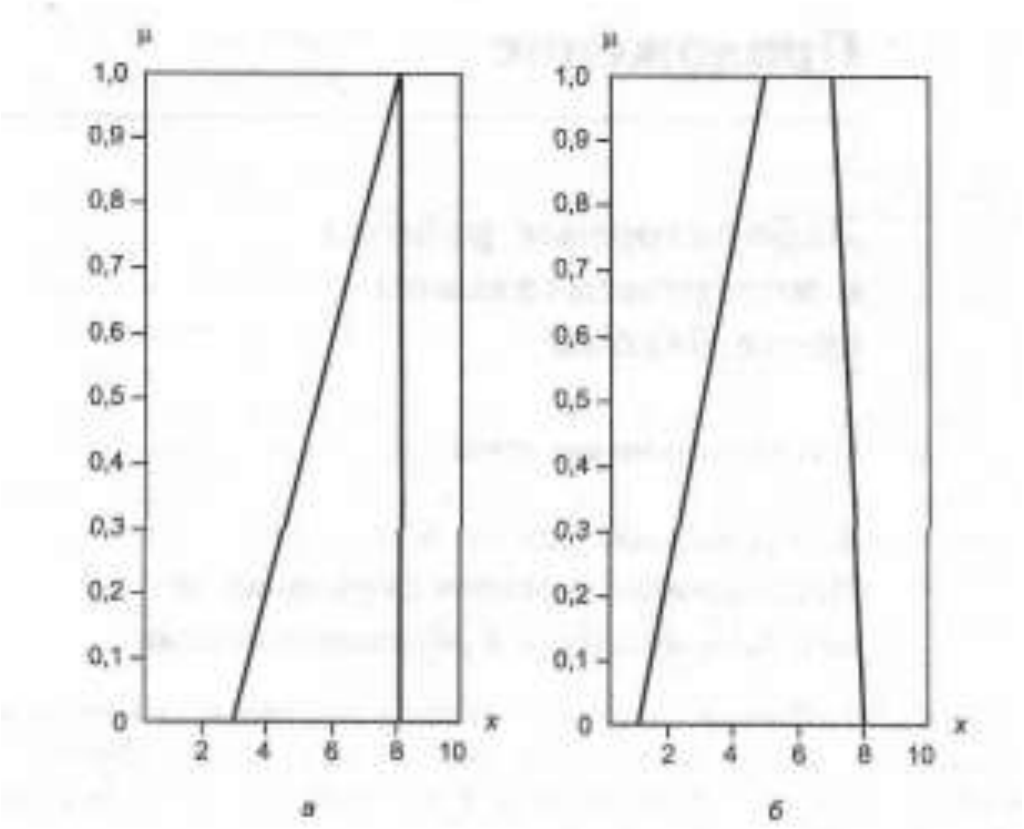


Рис. П1 . Трикутна (*а*) та трапецієподібна (*б*) функції приналежності

$$f(x,a,b,c) = \begin{cases} 0, x < a, \\ \dfrac{x-a}{b-a}, a \le x \le b, \\ \dfrac{c-x}{c-b}, b \le x \le c, \\ 0, x > c. \end{cases}$$

Далі розглянемо приклади використання різних ФП у системі.

Приклади є фрагментами програм і коментарів мовою пакету *Matlab* .

Приклад П1. Програма використання ФП trimf .

x = 0 : 0,1: 10; *Задається базова безліч*

y = trimf (x , [3 6 8]) ; *Визначається трикутна ФП*

plot (x, y) ; *Виводиться графік функції*

xlabel (' trimf (x , P) , P = [3 6 8]') ; *Підписується графік під віссю абсцис*

Трапецієподібна ФП - ***trapmf*** *(**trap** ezoid **m** embership **f** unction)* – відрізняється від попередньої функції лише тим, що має верхню основу.

Опис функції:

$$y = trapmf\ (x,\ [\ a\ b\ з\ d\ ]),$$

де параметри *a* та *d* - нижню основу трапеції;

b і *з* - верхня основа трапеції (рис. П1, *б)*.

Аналітичний запис трапецієподібної функції має вигляд:

$$f(x,a,b,c,d)=\begin{cases}0,\ x<a,\\ \dfrac{x-a}{b-a},\ a\le x<b,\\ 1,\ b<x\le c,\\ \dfrac{d-x}{d-c},\ c<x\le d,\\ 0,\ x>d.\end{cases}$$

Одна з основних переваг трикутних і трапецієподібних ФП – їхня простота. На основі функції розподілу Гауса можна побудувати ФП двох видів: просту функцію приналежності Гауса та двосторонню, утворену за допомогою різних функцій розподілу Гауса. Перша з них позначається ***gaussmf*** , а друга - ***gauss 2 mf*** .

Опис функції:

$$y = gaussmf\ (x\ ,\ [\ \sigma,\ c\ ])\ .$$

Симетрична функція Гауса залежить від двох параметрів *σ* та *c* (рис. П.2, *а):*

$$f(x,\sigma,c)=e^{\frac{-(x-c)^2}{2\sigma^2}}.$$

Приклад П2. Програма використання ФП gaussmf .

X = 0: 0,1: 10;

Y = gaussmf (x, [2 5]);

plot (x, y);

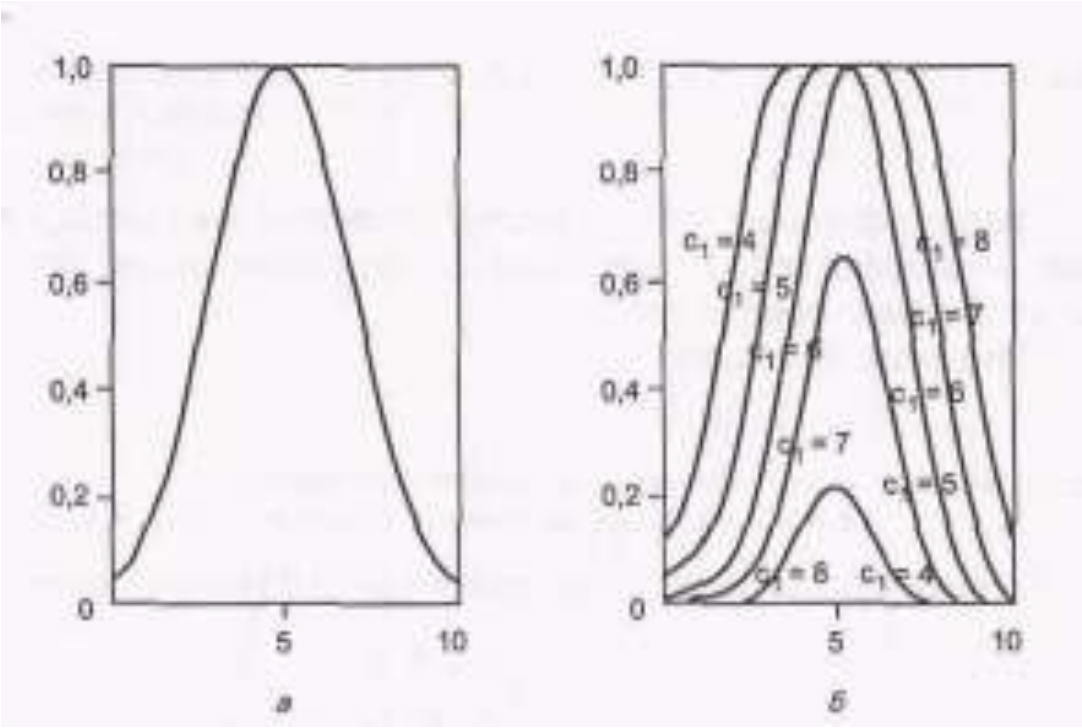


Рис. П2 . Проста (а) та двостороння *(б)* функції приналежності Гауса.

Опис функції:

$$y = gauss\ 2\ mf\ (\ x\ ,\ [\sigma_1\ ,\ з_1\ ,\ \sigma_2\ ,\ c_2\ ]).$$

Останній вираз є комбінацією двох різних функцій розподілу Гаусса. Перша визначається параметрами 1_i з 1_i задає форму лівої сторони, а друга (*параметри* $_2$, c_2) - правої сторони ФП.

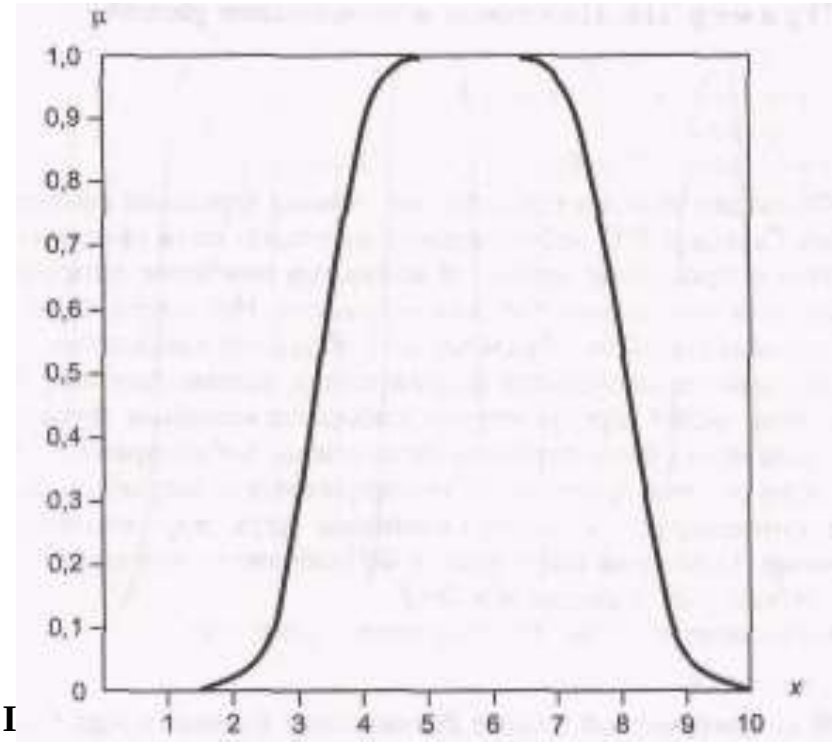
Якщо $з_1 < c_2$, то цьому випадку функція gauss 2 mf досягає свого максимального значення на рівні 1. Інакше – максимальне значення функції менше 1 (рис. П2, *б).*

Приклад ПЗ. Програма використання ФП gauss 2 mf .

```
x = (0: 0,1: 10)';
y 1 = gauss 2 mf ( x , [2 4 1 8]);
y2 = gauss 2 mf ( x , [2 5 1 7]);
y3 = gauss 2 mf ( x , [2 6 1 6]);
y4 = gauss 2 mf ( x , [2 7 1 5]);
y5 = gauss 2 mf ( x , [2 8 1 4]);
Plot ( x , [ y 1 y2 y3 y4 y5]);
```

Символ *«'»* у рядку визначення базової множини *x* показує транспонованість базової множини.

Наступною функцією, яка дозволяє представляти нечіткі суб'єктивні переваги, є ФП «узагальнений дзвін» та позначається ***gbellmf*** *(**g** eneralized **bell** shape **m** embership **f** unction).*



I

gbellmf , P = [2 4 6]

Рис. П3 . Функція приналежності «узагальнений дзвін»

Її відмінність від розглянутих раніше ФП полягає у додаванні третього параметра, що дозволяє здійснювати плавний перехід між нечіткими множинами.

Опис функції:

$$y = gbellmf\ (\ x\ ,\ [a\ b\ з]).$$

Функція «узагальнений дзвін» залежить від трьох параметрів і має наступний аналітичний запис:

$$f(x,a,b,c) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}},$$

де c – визначає розташування центру ФП; a та b - Надають вплив на форму кривої (мал. ПЗ).

Приклад П4. Програма використання gbellmf .

```
x = 0 : 0,1: 10;
y = gbellmf (x, [2 4 6]);
plot (x , y);
xlabel ( ' gbellmf , p = [2 4 61 ] ').
```

Функції приладдя на основі функції розподілу Гауса і ФП “узагальнений дзвін” відрізняються гладкістю та простотою запису і є найбільш використовуваними при описі нечітких множин. Незважаючи на те, що гаусові і дзвоноподібні ФП мають властивість гладкості, вони не дозволяють формувати асиметричні ФП. Для цього передбачено набір сигмоїдних функцій, які можуть бути відкриті або зліва, або праворуч залежно від типу

функції. Симетричні та закриті функції синтезують з використанням двох додаткових сигмоїдів. Основна сигмоїдна ФП позначається ***sigmf*** , а додаткові – ***dsigmf*** і ***psigmf*** .

Опис основної сигмоїдної функції: *y = sigmf (x, [a c]).*

В аналітичній формі сигмоїдна функція ***sigmf*** записується наступним чином:

$$f(x,a,c)=\frac{1}{1+e^{-a(x-c)}}.$$

Залежно від знака параметра *a* ФП, що розглядається, буде відкрита або праворуч або зліва (рис. П4, *а*), що дозволить застосовувати її при описі таких нечітких понять, як «дуже великий», «вкрай негативно» та ін.

Опис додаткової сигмоїдної функції:

$$y = dsigmf\ (x\ ,\ (a_1, c_1, a_2, з_2])).$$

ФП ***dsigmf*** залежить від чотирьох параметрів a_1, c_1, a_2 та $з_2$ і визначається як різницю двох сигмоїдних функцій: $f\ (x, a_1, c_1)$ - $f\ (x\ , a_2, c_2)$ (рис. П4, *б*) .

Опис додаткової сигмоїдної функції:

$$y = psigmf\ (x\ ,\ [a_1, c_1, a_2, з_2]).$$

ФП ***psigmf*** , як і і попередня функція, залежить від чотирьох параметрів a_1, c_1, a_2, $з_2$ і визначається як добуток двох сигмоїдних функцій $f\ (x, a_1, з_1) \cdot f\ (x\ , a_2, з_2)$ (рис. П4, *в*) .

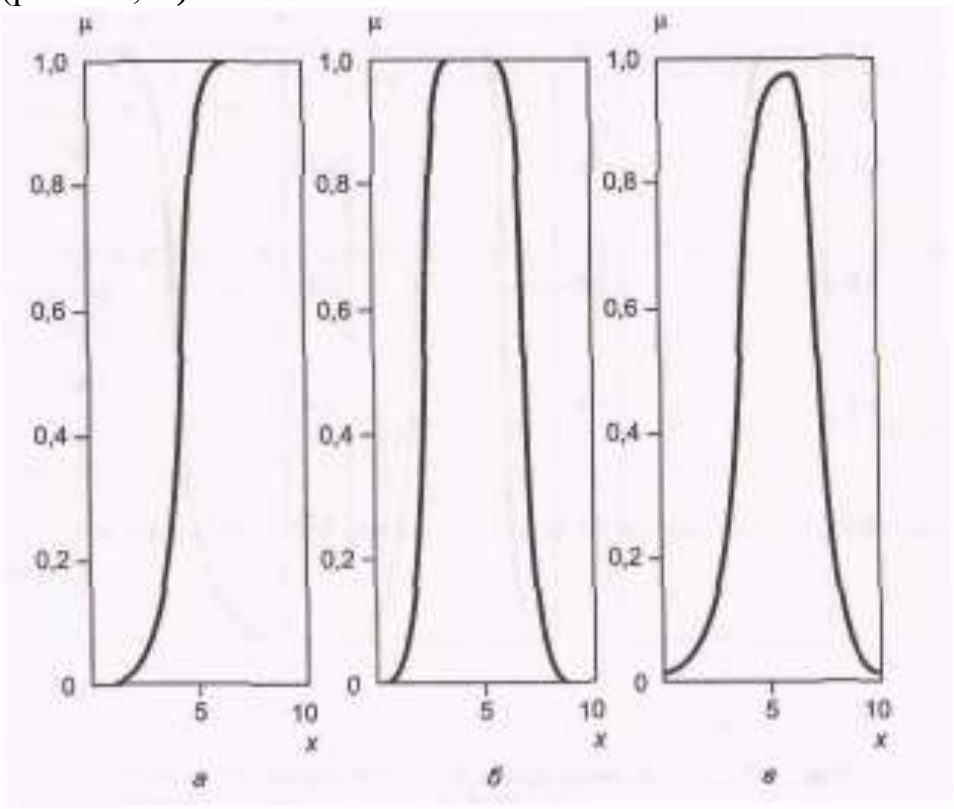


Рис. П4 . Сигмоїльні функції приладдя:
а – основна одностороння; *б* – додаткова двостороння;
в - додаткова несиметрична

Приклад П5. Програма використання функцій сигмоїдів.

```
x = 0: 0,1: 10;                визначається базова множина
subplot (1, 3, 1);             формується матриця графіків (3 ×1)
                               перший елемент – поточний
y = sigmf ( x , [2 4]);
plot (x, y);                   виводиться графік у перший елемент матриці
xlabel (' sigmf , P = [2 4]')
subplot (1, 3, 2);             вибирається другий поточний елемент
y = dsigmf ( x , [5 2 5 7]);
plot (x, y);                   виводиться графік у другий елемент матриці
xlabel ( ' dsigmf , P = [5 2 5 7]')
subplot (1, 3, 3);             вибирається третій поточний елемент
y = psigmf ( x , [2 3 -5 8]);
plot (x, y);                   виводиться графік у третій елемент матриці
xlabel (' psigmf , P = [2 3 -5 8 ] ');
```

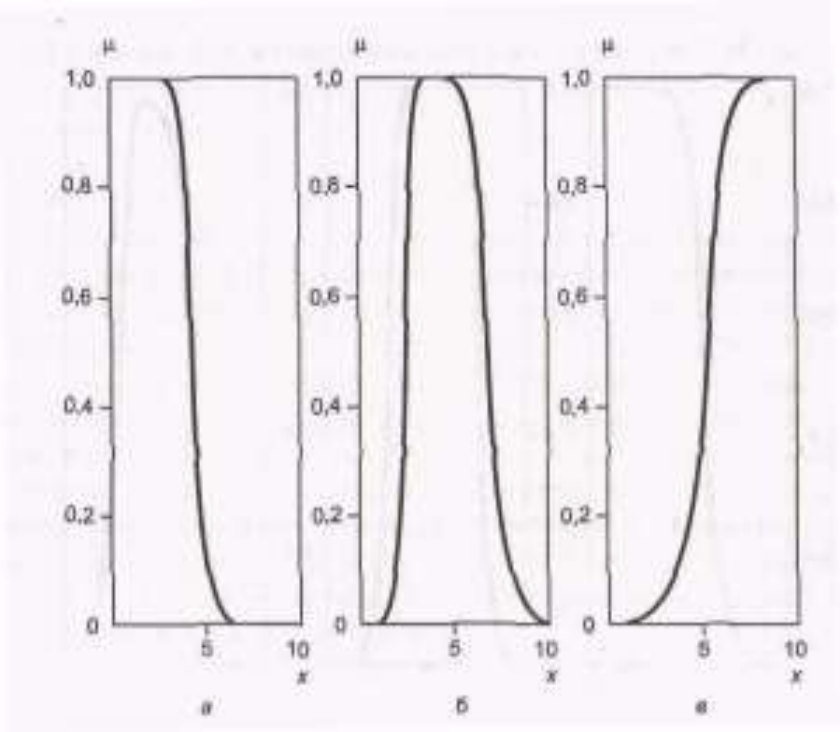


Рис. П5 . Поліноміальні функції приладдя:
а - *Z* -функція; *б* - *PI* -функція; *в* – *S* -функція

Інструментарій нечіткої логіки (fuzzy logic toolbox) у складі *Matlab* дає можливість формування ФП на основі поліноміальних кривих. Відповідні функції називаються ***Z*** -функції *(**zmf**),* ***PI*** *-* функції *(**pimf**)* та ***S*** -функції *(**smf**).* Функція ***zmf*** є асиметричною поліноміальною кривою, відкритою зліва (рис. П5, *а),* функція ***smf*** – дзеркальне відображення функції ***zmf*** (рис. П5, *в).* Відповідно функція ***pimf*** дорівнює нулю в правому і лівому межах і набуває значення, що дорівнює одиниці, в середині деякого відрізка (рис. П5, *б*).

Опис функції:

y = zmf (x , [a b]).

Параметри *a* та *b* визначають екстремальні значення кривої (рис. П 5, *а).*

Опис функції:

y = pimf (x , [a b з d]).

Параметри *a* та *d* задають перехід функції у нульове значення, а параметри *b* і с - в одиничне (рис. П5 *б).*

Опис функції:

y = smf (x, [a b]).

Параметри *a* та *b* визначають екстремальні значення кривої (мал. П5, *в).*

Приклад П 6 . Програма використання поліноміальних кривих.

```
x = 0: 0,1: 10;
subplot (1, 3, 1);
y = zmf ( x , (3 7]);
plot (x, y);
xlabel ('zmf, P = [3 7]');
subplot (1, 3, 2);
y = pimf(x, [14510]);
plot (x, y );
xlabel ('pimf, P = [1 4 5 10]');
subplot (1, 3, 3);
y = smf (x, [18]);
plot(x, y);
xlabel ( ' smf , P = [ 1 8 ] ').
```

Крім розглянутих вище функцій, що дозволяють представляти нечіткі множини, *Mattab* є можливість формувати власні ФП чи модифікувати вбудовані.

Операції з нечіткими множинами . Виділяють три основні логічні операції з нечіткими множинами: кон'юнкцію, диз'юнкцію та логічне заперечення. У середовищі *Matlab* існує можливість визначати кон'юнктивні та диз'юнктивні оператори з погляду мінімаксної та ймовірнісної інтерпретацій.

Розглянемо мінімаксну інтерпретацію логічних операторів, де кон’юнктивний оператор представляє перебування мінімуму – min (рис. П6, *а)* , а диз'юнктивний – максимум – max (рис. П6, *б).*

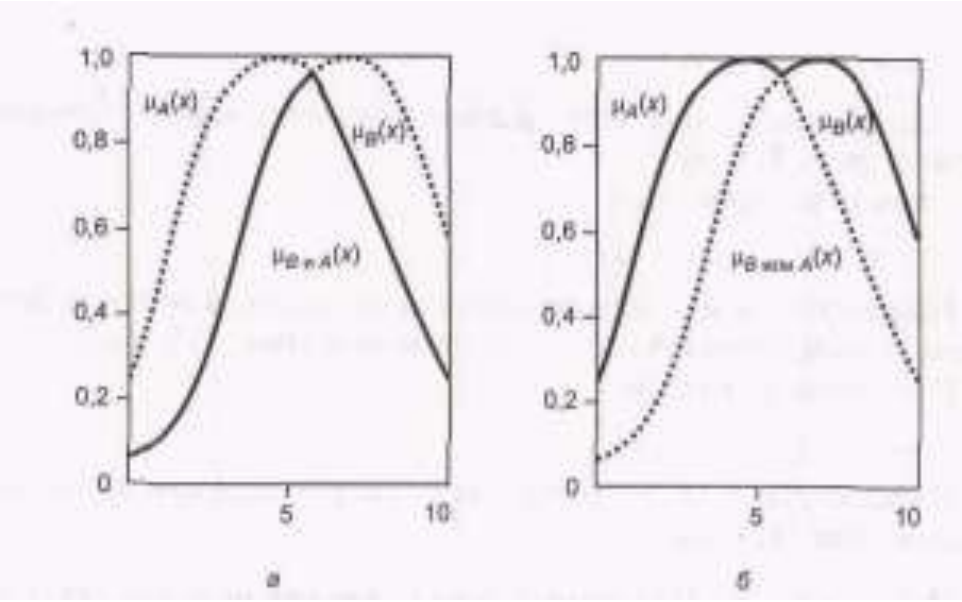


Рис. П6. Перетин (*а*) та об'єднання (*б*) нечітких множин (мінімаксна інтерпретація)

Опис кон'юнктивної функції: *y = min ([y 1 ; y 2]).*

Опис диз'юнктивної функції: *y = max ([y 1 ; y 2]).*

Параметри *y 1* і *y 2* є вихідними ФП. Функція min працює зі списком ФП. У *Matlab* список оформляється квадратними дужками, а елементи списку поділяються крапкою з комою.

Приклад П7. Програма використання операцій min та max .

```
x = 0: 0,1: 10;
subplot (1, 2, 1);
y1 = gaussmf (x, [3 5]);
y 2 = gaussmf (x, [3 7]);
y 3 = min ([ y 1; y 2]);
plot ( x , [ y 1; y2], ':');   побудова вихідних ФП пунктирною лінією
hold on ;                      включення механізму додавання кривої до поточного
                               графік
plot ( x , y3);
hold off ;                     вимкнення механізму додавання кривої у поточний
                               графік
subplot (1, 2, 2);
y4 = max ([ y 1; y2]);
plot(x, [y1; y 2], ':');
hold on;
plot (x, y4);
hold off.
```

Пунктирною лінією на графіках зображені вихідні ФП, а суцільною лінією – результат дії логічних операторів.

Мінімаксна інтерпретація є найпоширенішою при побудові нечітких систем. Проте, практично досить часто використовується альтернативна

ймовірнісна інтерпретація кон'юнктивних і диз'юнктивних операторів. *Matlab* містить відповідні функції.

В рамках даної інтерпретації кон'юнктивний оператор є оператором обчислення твору алгебри – ***prod*** (рис. П7, *а*), а диз'юнктивний оператор - оператор обчислення алгебраїчної суми - ***p r o b o r*** (Мал. П7, *б*).

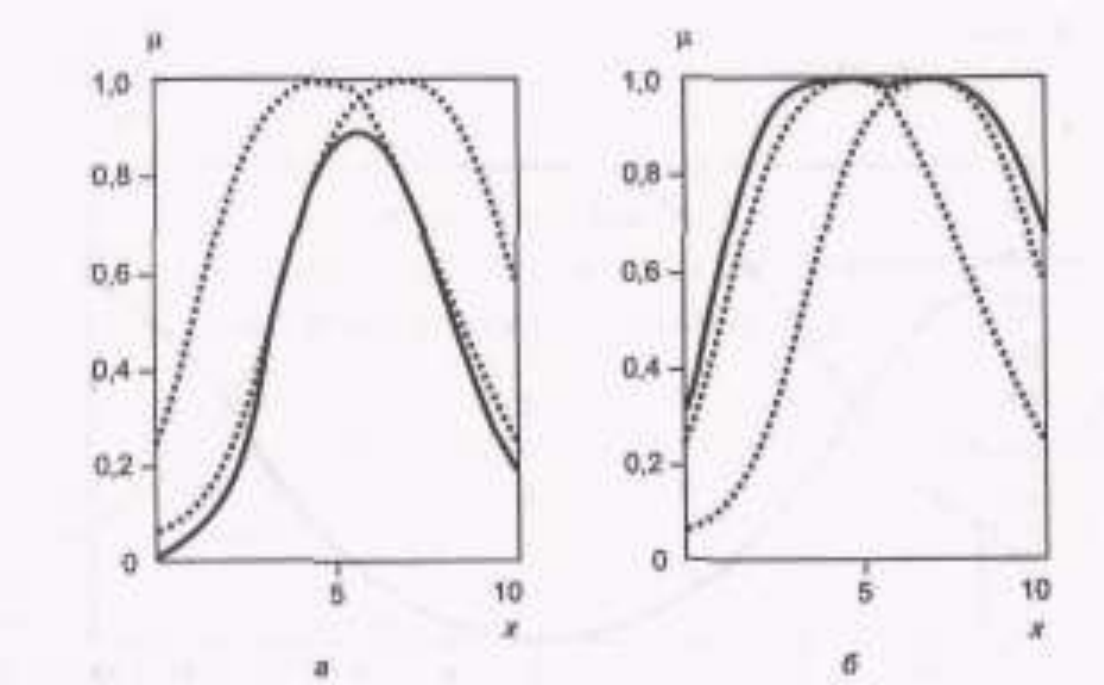


Рис. П7. Перетин (*а*) та об'єднання *(б)* нечітких множин (імовірнісна інтерпретація)

Опис функції: $y = prod([y_1; y_2])$

Опис функції: $y = probor([y_1; y_2])$.

Параметри y_1 і y_2 є вихідними Ф П

Приклад П8. Програма використання ймовірнісних операторів кон'юнкції та диз'юнкції.

```
x = 0: 0,1: 10;
subplot (1, 2, 1);
y1 = gaussmf (x, [3 5]);
y2 = gaussmf (x, [3,7]);
y 3 = prod ([y1; y2]);
plot ( x , [ y 1; y2], ':') ;
hold on;
plot(x, y3);
hold off;
subplot (1, 2, 2);
y4 = probor ([y1; y2]);
plot ( x , [ y 1; y 2], ':');
hold on;
plot(x, y4);
hold off .
```

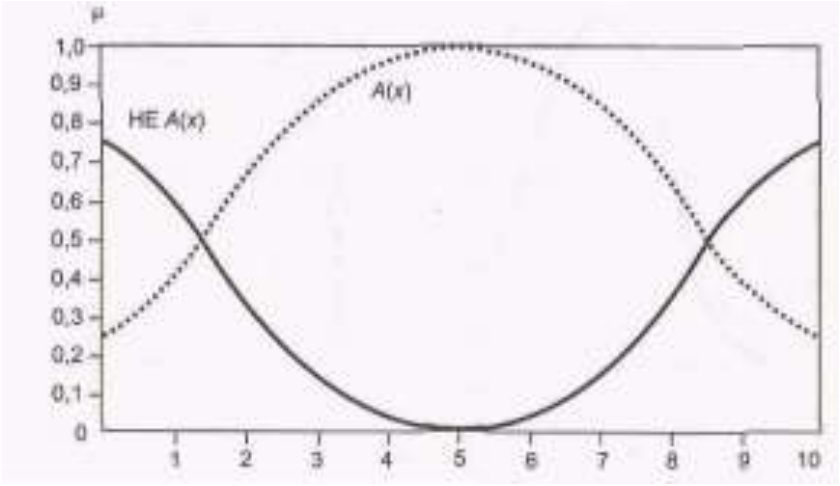


Рис. П8. Доповнення нечіткої множини.

Доповнення нечіткої множини є не що інше, як математичне уявлення вербального виразу «НЕ *A* » (рис. П8), де *A* - нечітка безліч, що описує деяке розмите судження.

Опис функції доповнення: $y = 1 - y^*$, де y^* - Вихідна ФП.

Приклад П9. Програма використання операції доповнення.

```
x = 0: 0,1: 10;
y 1 = gaussmf ( x , [3 5]);
y = 1 – y 1;
plot ( x , y1, ':');
hold on;
plot(x, y);
hold off.
```

ивчити метод побудови нечіткої системи засобами інструментарію нечіткої логіки (ІНЛ).

2. Короткі відомості з теорії

У складі *Matlab* є п'ять основних засобів графічного інтерфейсу користувача (ГІП), які забезпечують доступ до ІНЛ: редактори системи нечіткого виведення (СНО), функції належності, правил виведення, а також засоби перегляду правил та поверхні виведення. Ці кошти пов'язані між собою динамічно та вироблені зміни в одному з них спричиняють зміни в інших.

Редактор СНО надає можливість формування проектованої системи на високому рівні абстракції: кількість вхідних та вихідних змінних, найменування змінних.

Редактор функцій власності (ФП) використовується визначення форми ФП, асоційованих з кожної змінної.

Редактор правил виводу застосовується для редагування списку правил, які визначають поведінку системи, що проектується.

Засіб перегляду правил виведення використовується з метою діагностики і може показувати, наприклад, активність правил чи форму впливу окремих ФП на результат нечіткого виведення.

Засіб перегляду поверхні виводу використовується для відображення залежності виходу від одного або двох входів системи. Іншими словами, воно генерує та виводить карту поверхні виведення розробленої СНО.

Редактор СНО. Побудова нечітких систем по Мамдані.

Для побудови створюваної системи у командному рядку основного вікна *Matlab* необхідно набрати команду ***fuzzy*** . Вікно редактора нової СНО містить вхідну, позначену *input 1* і вихідну - *output 1* змінні. За замовчуванням ІНЛ пропонує створювати СНО типу Мамдані.

Щоб додати нову змінну, необхідно вибрати в меню ***Edit*** відповідний пункт (для вхідної змінної – ***Add input*** **,** на вихідний – ***Add output***) **.** Зміна назви змінної відбувається за кроками.

Крок 1. Відзначається змінна, яку потрібно перейменувати.

Крок 2 У полі редагування змінюється назва змінної за промовчанням на ім'я, запропоноване користувачем.

Збереження проектованої системи у робочий простір середовища *MATLAB* (у змінну) виконується за допомогою пункту меню ***File – Save to workspace as ...*** В цьому випадку дані зберігаються до закінчення сеансу роботи з *Matlab* . Для збереження даних на диску після закінчення сеансу роботи застосовується відповідний пункт того самого меню ***Save to disk as ...***

Редактор ФП . Наступним кроком у побудові нечіткої моделі засобами ІНЛ є асоціювання набору ФП з кожною вхідною та вихідною змінною. Ця операція проводиться у редакторі ФП трьома способами, активізувати який можна:

- вибором в меню ***View*** пункту ***Edit Membership Functions...*** *;*
- подвійним клацанням миші на зображенні відповідної змінної (вхідний або вихідний);
- набором у командному рядку оператора ***mfedit*** **.**

За допомогою редактора ФП можна відображати і редагувати будь-які ФП, асоційовані (пов'язані) з усіма вхідними та вихідними змінними СНО, що розробляється.

Зв'язування ФП з ім'ям змінної відбувається так:

- вибирається змінна на ім'я з набору графічних об'єктів вікна редактора ФП;
- вказується діапазон зміни значень для базової та видимий діапазон для поточної змінних;
- у меню ***Edit*** вибирається пункт ***Add MFs ...*** У вікні вибирають вид ФП та їх кількість.

Редагують ФП поточної змінної двома способами: використовуючи графічне вікно ФП або змінюючи характеристики ФП (найменування, тип та

числові параметри). При виборі необхідної ФП у графічному вікні допускається плавна зміна кривої за допомогою миші.

Таким чином, при побудові СНО необхідно за допомогою редактора ФП визначити відповідні функції кожної з вхідних і вихідних змінних.

Редактор правил виводу. Після того як зазначено кількість вхідних та вихідних змінних, визначено їх найменування та побудовано відповідні ФП, до СНО необхідно включити правила виведення. Для цього у меню ***View*** вибирається пункт ***Edit Rules ...*** або в командному рядку *Matlab* набирається команда ***ruleedit .***

Ґрунтуючись на описах вхідних та вихідних змінних, визначених у редакторі ФП, редактор правил виведення формує структуру правила автоматично. Від користувача потрібно лише зв'язати значення вхідних та вихідних змінних, вибираючи зі списку заданих раніше ФП та визначити логічні зв'язки між ними. Також допускається використання логічного заперечення (НЕ) та зміна ваги правил в діапазоні від 0 до 1.

Правила виводу можуть відображатись у вікні у різних форматах, які визначаються шляхом вибору відповідного пункту підменю ***Format*** меню ***Options*** . За замовчуванням використовується *розширений* формат відображення правил виводу (verbose form):

If (input_1 is[not] mf_1j $_1$) <and, or>...(input_i is[not] mf_ij $_i$)...<and,or>
(input_n is[not] mf__nj $_n$) then
(output_1 is[not] mf_n + 1j $_{n+1}$) <and, or>...
(output_k is[not] mf_k + nj $_{k+n}$) <and, or>... (output_m is[not] mf_m + nj $_{m+n}$)
(w),

де *i* – номер вхідної змінної;
j $_i$ – номер ФП *i* – й змінної;
k – номер вихідний змінної;
n – кількість вхідних змінних;
m – кількість вихідних змінних;
w - вага правила.

(Кругі дужки містять у собі обов'язкові параметри, квадратні – необов'язкові, а кутові – альтернативні параметри (один на вибір)) .

Крім формату за замовчуванням, існують ще два види форматів відображення правил: *символьний* (symbolic form) та *індексний* (indexed form). Символьний формат має такий вигляд:

(input _ 1 <~=,==> mf _ 1 j $_1$)<&, | >...
(input _ i <~=,==> mf _ ij $_i$) ... <&, | >
(input _ n <~=,==> mf _ nj $_n$) = >
(output _1<~=,==> mf _ n + 1 j $_{n+1}$)...<&, | >
(output _ k <~=,==> mf _ k + nj $_{k+n}$) <&, | >...
(output _ m <~=,==> mf _ m + nj $_{m \neq n}$) (W)

Відмінність символьного формату від розширеного полягає в тому , що замість словесної інтерпретації зв'язок використовує символьна (символи «&» і «|» – відповідно визначають логічне **І** та логічне **АБО** , символ «~» – логічне

заперечення, а символ «=> » є роздільником умовної та заключної частин правила (антецендента та консеквенту).

Загальний опис правила виведення в індексному форматі може бути поданий у такому вигляді:

[-]1 j_1 …[-] ij_i …[-] nj_n [-] $n+1$ j_{n+1} …[-] $k + nj_{k+1}$ …[-] $m + nj_{m+n}$ (w):<1,2>.

Тут порядок слідування чисел відповідає черговості змінних, причому символ « **,** » поділяє правило на умовну і заключну частини. До двокрапки записується порядковий номер відповідної ФП, після двокрапки – вид логічного зв'язування («1» – логічне І, «2» – логічне АБО). Логічне заперечення визначається символом «–».

Після визначення правил виведення в однойменному редакторі можна стверджувати, що СНО повністю створено.

Приклад П10. Створення СНО.

Розглянемо таку ситуацію. Необхідно оцінити ступінь інвестиційної привабливості конкретного бізнес-проекту на підставі даних про ставку дисконтування та період окупності.

Крок 1 . Викликаємо редактор для створення СНО, набираючи у командному рядку ***fuzzy*** . Додаємо вхідну змінну за допомогою вибору меню ***Edit*** пункту ***Add input*** **.** У результаті отримуємо наступну структуру СНО: два входи, механізм нечіткого виведення по Мамдані, один вихід. Оголошуємо першу змінну як *discont* , а другу – *period* , які відповідно представлятимуть ставку дисконтування та період окупності бізнес-проекту. Найменування вихідної змінної, на підставі якої приймається рішення про рівень інвестиційної привабливості бізнес-проекту, задається як *rate* . Збережемо створювану модель під ім'ям *Invest* . На рис. П9 представлено поточний стан вікна редактора СНО.

Крок 2. Кожний вхідний та вихідний змінної поставимо у відповідність набір ФП. Ця процедура реалізується у редакторі ФП. Для *discont* визначаємо діапазон базової змінної (Range) від 5 до 50 (одиниця вимірювання - відсотки). Такий самий діапазон вибираємо для її відображення (Display Range) . Додамо три ФП, тип яких **–** ***trimf*** . Послідовно виділяючи мишею окремі ФП, надамо найменування **–** *small , middle , big* відповідно невеликій, середній та великій ставці дисконтування. Вікно редактора ФП у стані показано на рис. П10. Змінний *период* діапазон базової змінної визначений рівним [3, 36] (одиниця виміру **–** місяці), поставлені у відповідність три ФП типу *gaussmfc* найменуваннями **–** *short , normal , long* . Таким чином, змінна терміну окупності бізнес-проекту прийматиме наступні значення: короткий, звичайний та тривалий термін окупності.

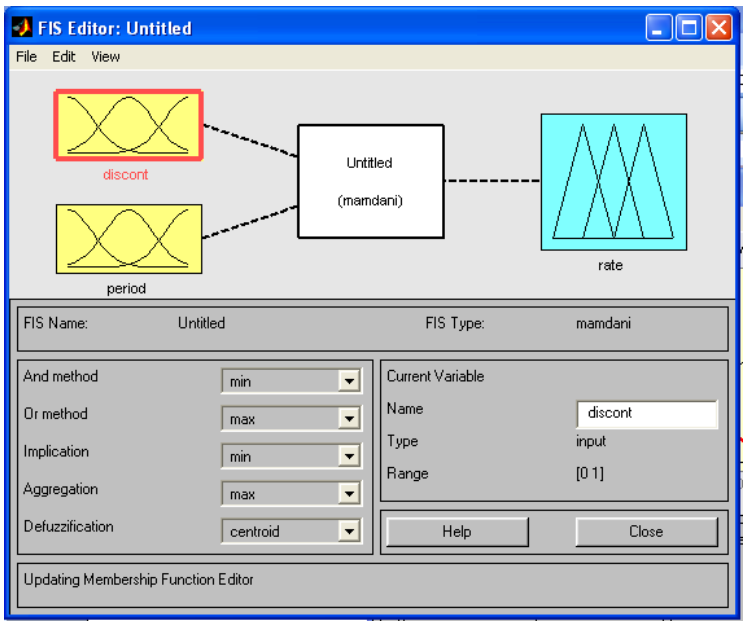


Рис. П9. Вікно редактора системи нечіткого виводу.

Нарешті, для змінної *rate* визначаємо: базова змінна змінює значення в діапазоні [0, 1], семантика описується трьома ФП типу ***trimf*** 'з найменуваннями: *bad* , *normal* , *good* .

Крок 3. Заключним етапом побудови СНО є визначення набору правил, що задають зв'язок вхідних змінних із вихідними. Для цього в редакторі правил виводу визначимо:

ЯКЩО *discont* = *small* І *period* = *short* ТО *rate* = *good*
ЯКЩО *discont* = НЕ *small* І *period* = *long* ТО *rate* = *bad*
ЯКЩО *discont* = *middle* І *period* = *normal TO rate* = *normal*
ЯКЩО *discont* = *big* І *period* = *short* ТО *rate* = *normal*

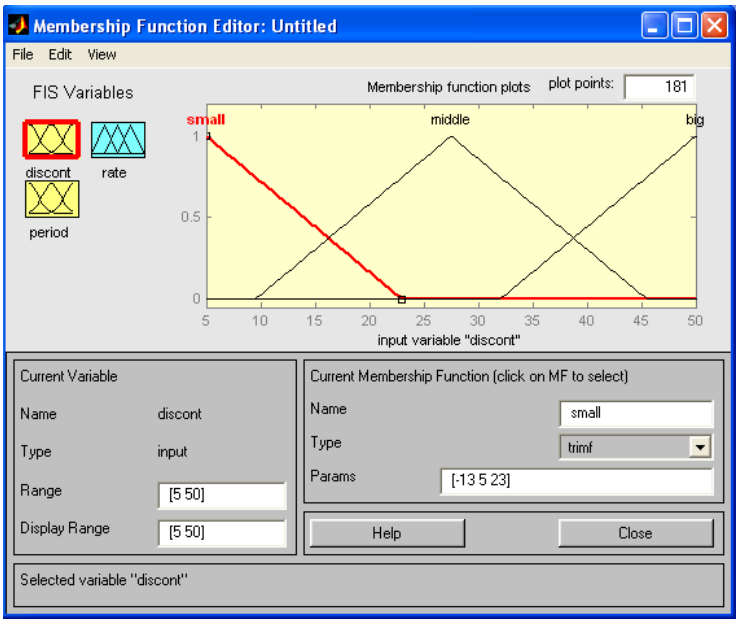


Рис. П10. Вікно редактора ФП

Поточний стан вікна редактора правил виведення показано на рис. П11. У розширеному форматі відображення зазначені правила виведення надаються таким чином:

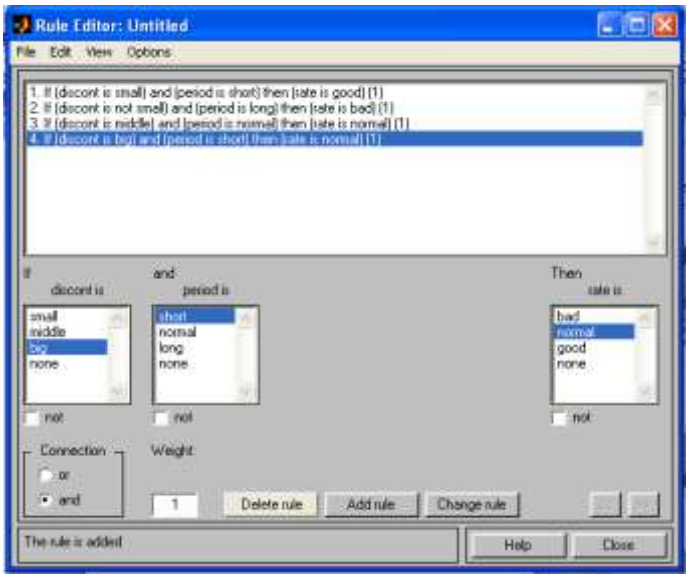


Рис. 11. Вікно редактора правил виводу

if(discont is small) and (period is short) then (rate is goad) (1)
if(discont is not small) and (period is long) then (rate is bad) (1)
if(discont is middle) and (period is normal) then (rate is normal) (1)
if(discont is big) and (period is short) then (rate is normal) (1)

При зміні формату на символьні правила виведення матимуть вигляд:
(discont == small) & (period == short) => (rate == good) (1)
(discont ~= small) & (period == long) => (rate == bad) (1)
(discont == middle) & (period == normal) => (rate== normal) (1)
(discont == big) & (period = = short) => (rate == normal) (1)

Нарешті, те саме, але в індексному форматі:

11,3(1) : 1
-13,1(1) : 1
22,2(1) : 1
31,2(1) : 1

Засіб перегляду правил виведення. Даний засіб перегляду правил виводу дозволяє відобразити процес нечіткого виводу та отримати результат. Головне вікно засобу перегляду складається з кількох графічних вікон, що розташовуються по рядках та стовпцях. Кількість рядків відповідає числу правил нечіткого висновку, а кількість стовпців – числу вхідних і вихідних змінних, заданих у СНО, що розробляється. Додаткове графічне вікно служить для відображення результату нечіткого виведення та операції дефазифікації. У кожному вікні відображається відповідна ФП, рівень її зрізу (для вхідних змінних) та вклад окремої ФП у загальний результат (для вихідних змінних).

У нижній частині головного вікна можна відобразити номери правил виведення в різних форматах виводу, позначаючи їх мишею. Для зміни формату в меню ***Options*** вибирається пункт ***Rule display format*** **.**

Зміна значень вхідних змінних допустимо двома способами:

1) шляхом введення у поле *Input* записи вхідного вектора, розмірність якого дорівнює кількості вхідних змінних;

2) клацанням миші в будь-якому графічному вікні, яке відноситься до вхідної змінної.

Вхідний вектор у кожному з цих варіантів визначення вихідних даних задаватиме набір червоних вертикальних прямих.

Для СНО, розглянутої у прикладі П10 , при вхідному векторі [15 10] (ставка дисконтування – 15 %, період окупності бізнес-проекту – 10 місяців) результат (ступінь інвестиційної привабливості) становитиме 0,585 (рис. П12 **).**

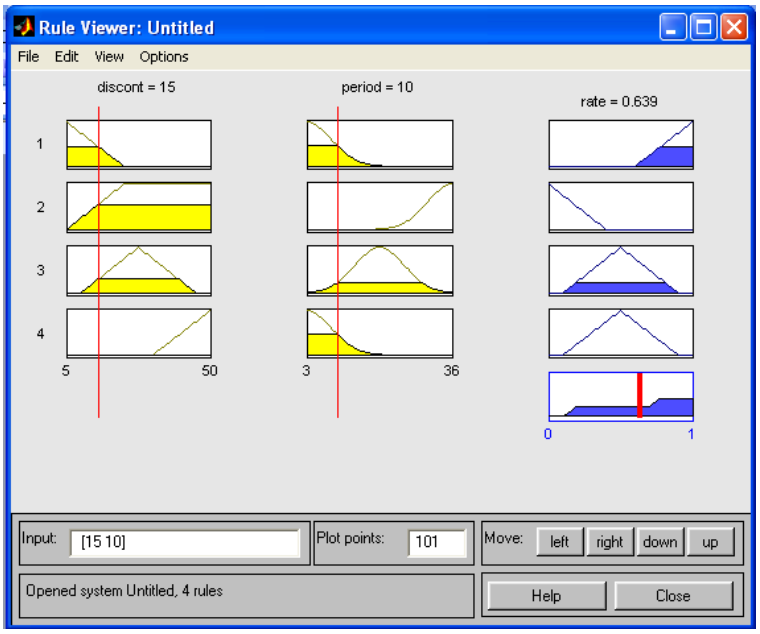


Рис. П1 2 . Вікно засобу перегляду правил виведення (Ctrl +5)

Засіб перегляду поверхні виводу. Засіб перегляду поверхні виводу дозволяє будувати тривимірну поверхню як залежність однієї із вихідних змінних від двох вхідних. Вибір вхідних і вихідних змінних здійснюється за допомогою спадних меню головного вікна програмного засобу, що розглядається. Кількість ліній, що виводяться по осях *X* і *Y* визначається полях введення *X grids* , *Y grids* . Поверхня виведення, що відповідає правилам виведення прикладу П10, показана на рис. П13.

Побудова нечітких систем типу Суджено.

Розглянемо побудову СНО двома редакторами – СНО та ФП. Для побудови СНО типу Суджено необхідно в меню ***File*** вибрати пункт ***New FIS -> Sugeno*** . Кількість вхідних та вихідних змінних визначається так само, як і при побудові СНО типу Мамдані.

Редактор ФП. Для СНО типу Суджено зміни стосуються лише схеми визначення ФП для вихідних змінних. ІНЛ у середовищі *Matlab* дозволяє

розробляти два види нечітких моделей. Перша модель – це нечітка модель Суджено нульового порядку. Нечітке правило виведення має такий вигляд:

if x is A and y is У then z = до ,

де *A* і *B* – нечіткі множини антецедента; *до* – чітко задана константа консеквенту.

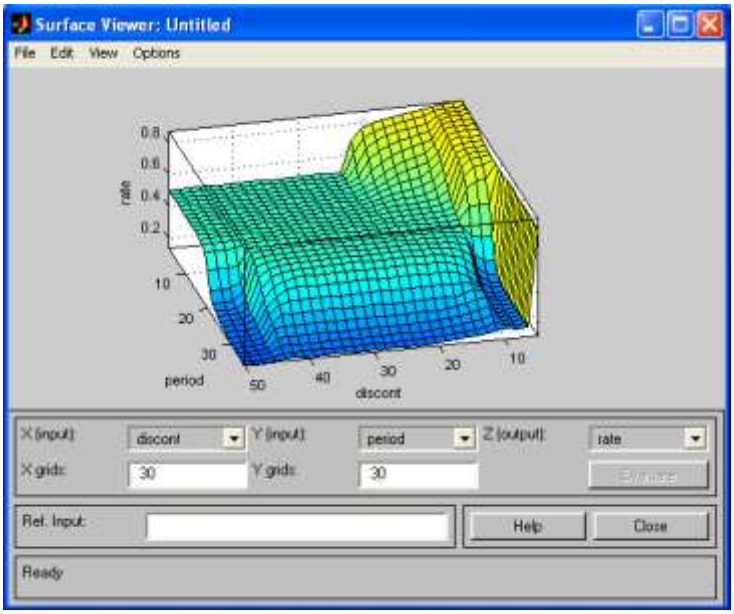


Рис. П13. Вікно перегляду поверхні рішень (Ctrl +6)

Для побудови такої моделі при додаванні ФП необхідно вибрати тип - константа (*constant*) і задати як параметр ФП чисельне значення відповідної константи. Друга модель - нечітка модель Суджено першого порядку. Для неї нечітке правило виведення записується так:

if x as A and y is У then z = p x + q y + r,

де *p, q* та *r* – константи.

У разі тип ФП – лінійна залежність *(linear).* Для визначення параметрів ФП необхідно ввести вектор, елементи якого відповідають чисельним значення констант консеквента.

Робота з редактором правил виведення, а також із засобами перегляду правил та поверхні виведення виконується аналогічно випадку побудови СНО по Мамдані.

Приклад нечіткого висновку Суджено з використанням нечіткої моделі нульового порядку і правил виведення, визначених вище, представлений на рис. П14 (вихідна змінна має три значення: *bad , normal , good ,* які задаються відповідно трьома константами – 0, 0.5, 1).

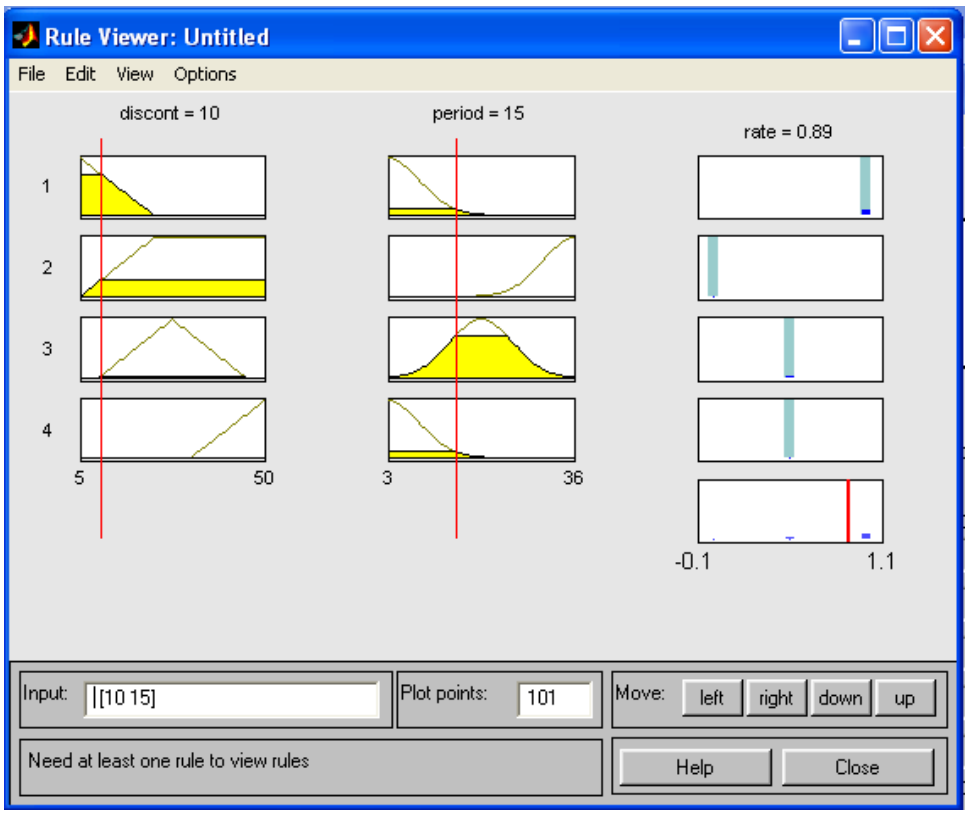


Рис. П 14. Вікно перегляду правил виведення (висновок щодо Суджено)

Індивідуальні завдання

1. Побудувати трикутну та трапецієподібну функцію приналежності.
2. Побудувати просту та двосторонню функцію приналежності Гауса, утворену за допомогою різних функцій розподілу.
3. Побудувати функцію приналежності «узагальнений дзвін», що дозволяє представляти нечіткі суб'єктивні уподобання.
4. Побудувати набір сигмоїдних функцій:

4.1. Основну односторонню, яка відкрита зліва чи праворуч;
4.2. Додаткову двосторонню;
4.3. Додаткову несиметричну.

5. Побудувати набір поліноміальних функцій приналежності (*Z*- , *PI*- та *S* -функцій).
6. Побудувати мінімаксну інтерпретацію логічних операторів з використанням операцій пошуку мінімуму та максимуму .
7. Побудувати ймовірнісну інтерпретацію кон'юнктивних та диз'юнктивних операторів.
8. Побудувати доповнення нечіткої множини, що описує деяке розмите судження, і є математичним описом вербального виразу, що заперечує цю нечітку множину.

За виконання пунктів 1 – 8 індивідуального завдання, значення змінних *a , b , c , d* і т.д. необхідно вибирати довільним чином.

9. Необхідно сформулювати абстрактну ситуацію, в галузі обчислювальної техніки або програмування та побудувати для неї нечітку систему, з використанням графічного інтерфейсу користувача, який забезпечує доступ до інструментарію нечіткої логіки та редактора системи нечіткого виведення. При цьому побудова нечіткої системи, для студентів з парними номерами за списком у журналі групи, має ґрунтуватися на принципі Мамдані, а для студентів з непарними номерами за списком у журналі групи повинні ґрунтуватися на принципі Суджено .

2. При виконанні пункту 1. індивідуального завдання задатись різними діапазонами зміни вхідних та вихідних змінних нечіткої системи, а також різними типами ФП .

3. Побудувати графічне відображення правил виведення та поверхні рішень, сформульованої абстрактної ситуації .

Зміст звіту

1. Тема лабораторної роботи.
2. Мета лабораторної роботи.
3. Індивідуальне завдання.
4. Результати виконання пунктів 1-8 індивідуального завдання.
5 . Висновки щодо лабораторної роботи.

Контрольні питання

1. Що таке нечітка множина і яка його основна відмінність від звичайної (чіткої) множини?
2. Що таке функція приналежності?
3. Які кон’юнктиві та диз'юнктивні оператори ви знаєте?
1. Яка структура типової системи нечіткого виведення?
2. У чому відмінність методу нечіткого висновку щодо Суджено від методу нечіткого висновку щодо Мамдані?
3. Як формуються антецеденти та консеквенти нечітких правил у *Matlab*?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту.

Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)
3. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.
4. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навчальний посібник. – Запоріжжя: ЗНТУ, 2008. – 341 с.
5. Асєєва Л.А. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки/ Л.А. Асєєва, О.М. Шушура //Телекомунікаційні та інформаційні технології. 2021. № 1 (70). – С. 88-95.
6. Методичні вказівки до виконання лабораторних робіт з дисципліни "Нечітке програмування" “Програмне забезпечення систем” усіх форм навчання / Уклад.: С.О. Субботін. – Запоріжжя: ЗНТУ, 2013. – 50 с.

Додаткова література з навчальної дисципліни

7. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.
8. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

9. Державна служба спеціального зв’язку та захисту інформації (ДСЗЗІ) [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua
10. Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін. Комплексні системи захисту інформації / Навчальний посібник. [Електронний ресурс]. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/