ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Безопасность информационных систем и сетей интернета вещей»
для студентов специальности 10.05.03 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2021

Составитель С.А. Ермаков

УДК 004.056.5

Методические указания к выполнению лабораторных работ по дисциплине «Безопасность информационных систем и сетей интернета вещей» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. С.А. Ермаков. Воронеж, 2021. 44 с.

Методические указания посвящены исследованию различных подходов к обеспечению безопасности сетей интернета вещей, на основе анализа рисков, и оценки защищенности IoT – сетей на базе аппарата теории нечётких множеств и нечёткой логики.

Методические указания подготовлены в электронном виде в текстовом редакторе MW-2016 и содержатся в файле Ермаков_ЛР_БИСиСИВ.docx.

Табл. 8. Ил. 27. Библиогр.:6 назв.

Рецензент д-р техн. наук, проф. А.Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А.Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

Лабораторная работа №1
Оценка защищенности группы устройств в Internet of Things – сети

Цель работы: Зная экспертные оценки, для каждого устройства и его протоколов безопасности, получить оценку защищенности IoT – сети для группы беспроводных соединений, используя механизм нечёткой логики. Анализ и выбор протоколов безопасности устройств в проектируемой сети.

Теоретические сведения

1. Internet of Things – это новый шаг в техническом прогрессе. Интернет вещей позволяет людям и вещам подключаться в любое время и в любом месте, используя различные коммуникационные сети. Происходит интенсивное развитие самоорганизующихся сетей связи, в которых абоненты не только люди, но и различные автоматические устройства, которые осуществляют информационное взаимодействие друг с другом без непосредственного участия человека в рамках межмашинной коммуникации [1]. В настоящее время уже можно увидеть, как различные устройства, работают без участия человека и соединены друг с другом посредством интернета. Примерами таких систем могу быть системы управления освещением, системы управления, систем автоматического полива, пожарные и охранные датчики, светофоры и т. д. [2].

К основной идеи Интернета вещей можно отнести организацию взаимодействия различных объектов в среде обитания человека, передаче информации, генерируемой этими вещами и обеспечении надежной связи. Взаимодействие вещей осуществляется через существующие и развивающиеся информационно-коммуникационные технологии [2].

2. Различные беспроводные соединения и протоколы безопасности. Зачастую все IoT-сети состоят из группы разнородных устройств, которые имеют различные виды бес-

проводных соединений, например, работающие по технологии Wi-Fi, Bluetooth, Z-wave, ZigBee, NFC и другие. К тому же каждая беспроводная технология обладает различными типами протоколов безопасности, которые могут отличаться друг от друга. Это является большой проблемой по оценке таких сетей [3].

В данной лабораторной работе рассматривается платформа M2M-сервисов для реализации технологии «Умный дом» с использованием разнородных устройств. Важно понимать, что множество протоколов безопасности, которые используются для связи устройств в мультистандартной сети, имеют специфические требования и аспекты безопасности. Поэтому много внимания уделяется безопасности использования таких сетей.

Для расчета оценки защищенности устройств IoT-сетей необходимы входные значения защищенности каждого беспроводного соединения в этой сети. На данный момент исходными могут быть только экспертные оценки, которые не дают точного результата и находятся в диапазонах, тогда как нам необходимы точные оценки защищенности.

Методом опроса экспертов можно составлены таблицы с экспертными оценками защищенности:

Таблица 1.1 – Возможные протоколы безопасности беспроводных соединений в предложенной схеме умного дома

	Протоколы	Качественная оценка защищенности
Wi-Fi	WEP	Низкая
	WPA	Средняя
	WPA2	Высокая
Bluetooth	V2.0	Низкая
	V3.0	Средняя
	V4.0	Высокая
Z-Wave	S0	Низкая
	S2	Высокая
NFC	Mifare Classic	Низкая
	Mifare DESFire	Средняя

	NTAG413	Высокая

Таблица 1.2 – Оценки защищенности протоколов безопасности беспроводных соединений по технологии Wi-Fi

Версии протоколов безопасности	Оценка уровня защищенности
WEP	0-0.3
WPA	0.3-0.7
WPA2	0.7-1

Таблица 1.3 – Оценки защищенности протоколов безопасности беспроводных соединений по технологии Bluetooth

Версии протоколов Bluetooth	Оценка уровня защищенности
V 2.0	0-0.3
V 3.0	0.3-0.7
V 4.0	0.7-1

Таблица 1.4 – Оценки защищенности протоколов безопасности беспроводных соединений по технологии Z-Wave

Версии протоколов безопасности	Оценка уровня защищенности
S0	0-0.3
S2	0.3-1

Таблица 1.5 – Оценки защищенности типов NFC-чипов

Типы NFC-чипов	Оценка уровня защищенности
Mifare Classic	0-0.3
Mifare DESFire	0.3-0.7
NTAG413	0.7-1

Получив экспертные оценки для каждого беспроводного соединения необходимо дать качественные оценки каждому диапазону значений для дальнейшего использования этих данных.

Таблица 1.6 – Соотношение качественных и экспертных оценок

Уровень защищенности	Оценка уровня защищенности
Низкий	0-0.3
Средний	0.3-0.7
Высокий	0.7-1

Задачи

1. Изучить представленную информацию о сетях Интернета Вещей.
2. Используя экспертные оценки защищенности построить графики функций принадлежности нечетких множеств для каждого беспроводного соединения.
3. Используя полученные графики, сформировать искомую функцию принадлежности.
4. Создать решающие правила к входным данным (оценки экспертов), служащие для конвертации четких входных данных к нечёткому формату.
5. Получить точную оценку защищенности сети для группы беспроводных соединений с различными комбинациями протоколов.
6. Составить отчёт по пунктам 2-5.

Порядок выполнения работы

1. Изучить теоретическую часть данной работы и получить представление об IoT – сети и понятии экспертной оценки.
2. Построение графиков функции принадлежности нечётких множеств для каждого беспроводного соединения.
   2.1. Запустить САПР MatLab во вкладке APPS перейти во Fuzzy Logic Designer. (рис.1).
   2.2. Через вкладку Edit => Add Variable => Input добавить 4 входные переменные, которые соответствуют рассматриваемым беспроводным технологиям.
   2.3. Про именовать их Wi-Fi, Bluetooth, Z-Wave и NFC. Для этого одним кликом ЛКМ переходим к перемен-

ной, в поле Current Variable (Name) вводим название. Выполнить для каждой переменной.

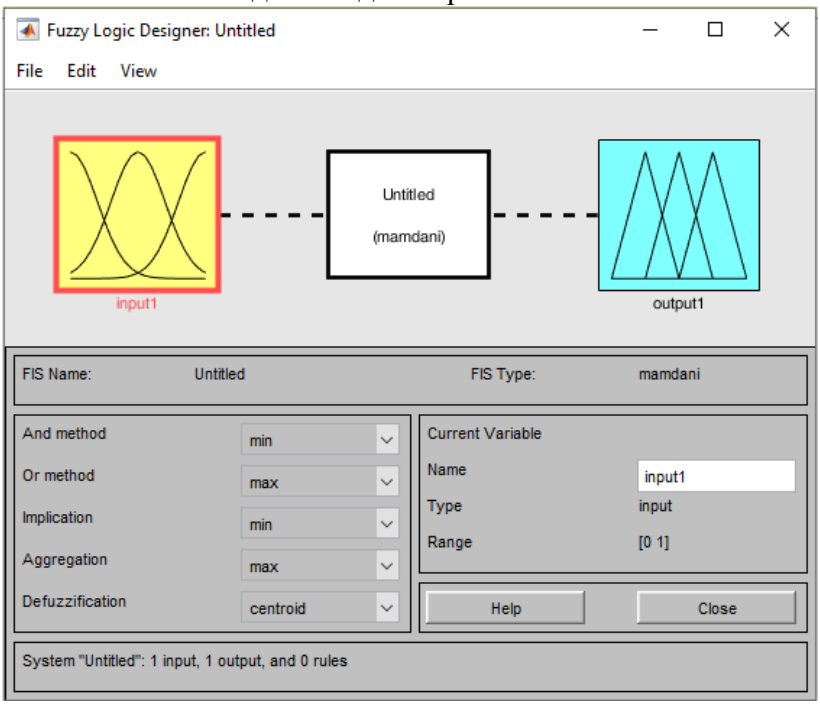

Рис.1 Главное окно Fuzzy Logic Designer.

2.4. Двойным нажатием ЛКМ по любой из переменных перейти в Membership Function Editor (рис. 2). Для каждой технологии через вкладку Edit => Add MFs… добавить Membership Function, MF type – trimf, a Number of FMs – равно количеству протоколов безопасности (например, для Wi-Fi значение равно 3).

2.5. В поле Membership function plots выбираем функцию и в полях Current variable и Current MF редактируем. Range для переменных с 3-мя протоколами [0 2], а для переменных с 2-умя [0 1]. Name соответствует протоколу, Type – trimf, Params заполняется исходя из теоретических материалов.

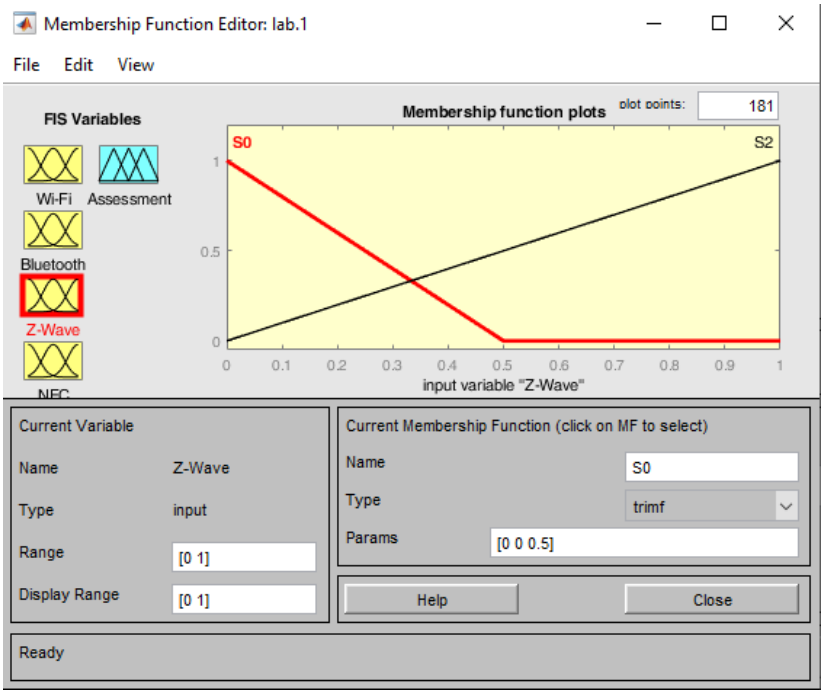

Рис. 2 Membership Function Editor.

3. Настройка искомой функции принадлежности.
   3.1. Выбрать output1 и переименовать в Assessment (Оценка) перейти в его настройки. Добавить 3 функции с названием Low, Middle, High.
   3.2. Range [0 1] для всех функций. Params для Low [0 0 0.5], для Middle [0 0.5 1], High [0.5 1 1]

4. Фазификация.
   4.1. Следующим шагом будет этап фазификации, который заключается в применении решающих правил к входным данным (оценки экспертов) и служит для конвертации четких входных данных к нечеткому формату.
   4.2. Через окно Membership Function Editor открыть вкладку Edit => Rules…, для настройки правил нужно выбрать протокол безопасности для одной из беспро-

водных технологий, остальным присвоить none, и согласно теории, Assessment присвоить нужную качественную оценку (рис.3). Нажать Add rule, повторить для всех протоколов безопасности.

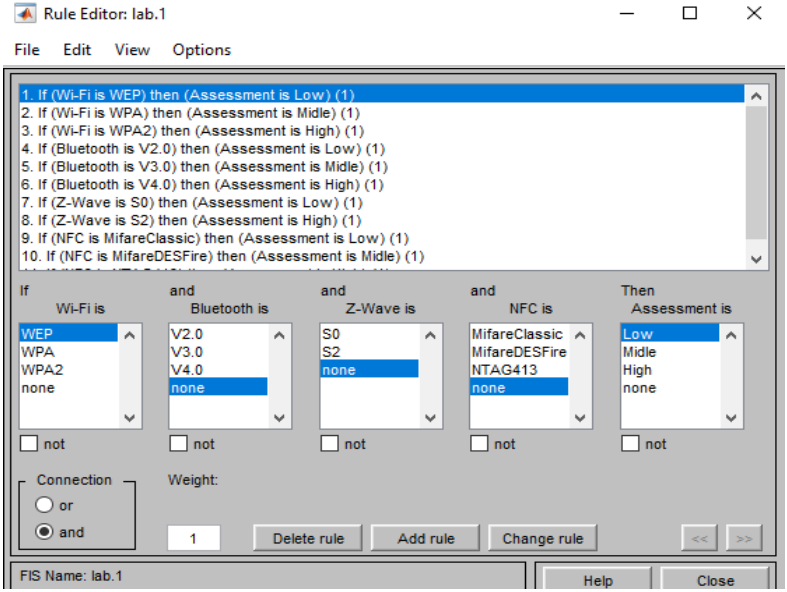

Рис.3 Настройка решающих правил Wi-Fi протокол WEP.

5. Получение точной оценки защищённости сети для группы беспроводных соединений с различными комбинациями протоколов.

5.1. Для этого в окне Rule Editor выбрать вкладку View => Rules. В открывшимся окне в поле Input ввести выбранные протоколы согласно таблице 2. Например: для комбинации протоколов WPA, V4.0, S2, NTAG413 (0 Вариант), Assessment(Оценка) = 0.837.

Таблица 2 – Определение входных значения для каждого протокола беспроводных соединений

Беспроводное соединение	Протокол	Входное значение
Wi-FI	WEP	0
	WPA	1

	WPA2	2
Bluetooth	V2.0	0
	V3.0	1
	V4.0	2
Z-Wave	S0	0
	S2	1
NFC	MifareClassic	0
	MifareDESFire	1
	NTAG413	2

5.2. Получить Assessment(Оценку) для всех комбинаций протоколов согласно вашему варианту, про ранжировать их и занести в отчёт.

Лабораторная работа №2
Оценка нечеткого риска для сети с различными комбинациями версий протоколов безопасности

Цель работы: Используя оценки защищённости групп устройств, из 1 лабораторной работы, получить оценку нечёткого риска, для устройств, использующих разные протоколы безопасности и работающих на одной и той же беспроводной технологии

Теоретические сведения

В классическом понимании риск определяется исходя из двух факторов: вероятность реализации угрозы и ущерб, нанесенный владельцу информации от реализации угроз:

$$R = P(U) \times U, \quad (1)$$

где R - риск, P - вероятность реализации угрозы, U - ущерб от реализации деструктивного действия.

В данном случае, нельзя применять риск в классическом виде, так как система, которую мы хотим оценить, является сложной. В данных условиях отсутствует информация об ущербах. Поэтому необходимо предложить альтернативный вариант расчета риска.

В данной лабораторной работе необходимо ввести такое понятие, как нечеткий риск, который будет являться, некоторой эмпирической мерой защищенности сети и будет зависеть от нее.

Используя результаты, полученные в первой лабораторной работе, можно разбить таблицу ранжирования комбинаций протоколов беспроводных соединений на группы и дать каждой группе качественную оценку защищенности для дальнейшего вычисления нечетких рисков для различных комбинаций, которые могут быть использованы при реализации IoT-сети.

Комбинации протоколов для удобства использования необходимо разбить на группы с качественными оценками типа: недопустимый уровень защищенности, низкий уровень защищенности, умеренный уровень защищенности, средний уровень защищенности и высокий уровень защищенности.

Таблица 3.1 – Сопоставление оценок защищенности и уровня защищённости для заданных комбинаций протоколов в сети

Оценка защищенности сети	Уровень защищенности сети
1.00-0.75	Высокий
0.74-0.55	Средний

0.54-0.48	Умеренный
0.47-0.40	Низкий
0.39-0.00	Критический

Таблица 3.2 – Сопоставление качественных оценок уровня защищенности и нечеткого риска для заданных комбинаций протоколов в сети

Уровень защищенности	Нечеткий риск
Высокий	Низкий
Средний	Умеренный
Умеренный	Средний
Низкий	Высокий
Критический	Экстремальный

Задачи

1. Изучить понятие риска и нечеткого риска для группы устройств.
2. Дать качественную оценку защищённости группе устройств.
3. Сопоставить качественные оценки с нечётким риском для комбинаций протоколов.
4. Получить числовое значение нечёткого риска.
5. Получить риск для различных версий протоколов безопасности у устройств, работающих на одной и той же беспроводной технологии.
6. По выполненным пунктам 2-5 составить отчёт.

Порядок выполнения работы

1. По полученным данным в первой лабораторной работе дать качественную оценку для выхода Assessment (оценка защищенности) по таблице 3.1.

1.1. Пример для варианта №0:

Протоколы безопасности	Оценка защищенности	Качественная Оценка

1. WPA2 and V4.0 and S2 and NTAG413	0.837	Высокий уровень
2. WPA2 and V2.0 and S2 and NTAG413	0.5	Умеренный уровень
3. WPA and V3.0 and S2 and NTAG413	0.587	Средний уровень
4. WEP and V3.0 and S2 and NTAG413	0.5	Умеренный уровень
5. WEP and V3.0 and S0 and MifareClassic	0.413	Низкий уровень

2. По таблице 3.2 сопоставить качественные оценки с нечётким риском.

2.1. Пример для варианта №0:

Протоколы безопасности	Качественная Оценка	Нечёткий РИСК
1. WPA2 and V4.0 and S2 and NTAG413	Высокий уровень	Низкий уровень
2. WPA2 and V2.0 and S2 and NTAG413	Умеренный уровень	Средний уровень
3. WPA and V3.0 and S2 and NTAG413	Средний уровень	Умеренный уровень
4. WEP and V3.0 and S2 and NTAG413	Умеренный уровень	Средний уровень
5. WEP and V3.0 and S0 and MifareClassic	Низкий уровень	Высокий уровень

3. Численная оценка нечёткого риска.

3.1. Во Fuzzy Logic Designer создать новый проект, входными переменными так же, как и в лабораторной работе №1 будут: Wi-Fi, Bluetooth, Z-Wave, NFC. Current Variable, Membership Function заполнять по аналогии с предыдущей работай.

3.2. Выходной переменной будет нечёткий риск – RISK. Переменная должна содержать 5 функций, соответствующих нечёткому риску, определённому ранее. При-

своить им подходящие названия: Низкий уровень – Low, Умеренный уровень – Moderate, Средний уровень – Middle, Высокий уровень – High, Экстремальный уровень – Extreme (Рис. 4).

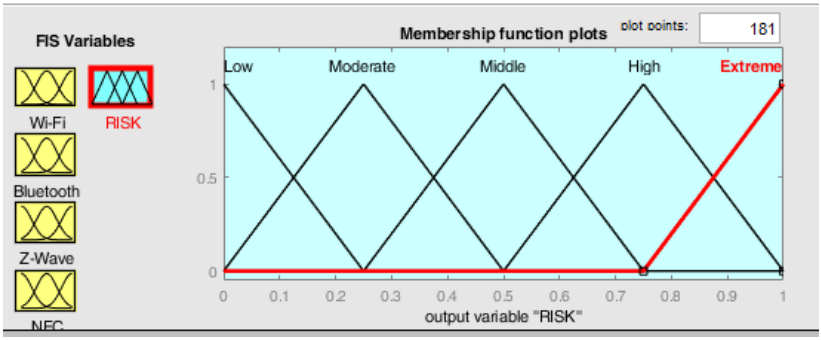

Рисунок 4 – Membership Function Editor.

3.3. Далее переходим в Rule Editor (из окна Membership Function Editor можно перейти нажатием Ctrl+3), для настройки решающих правил нужно выбрать протоколы безопасности для каждой комбинации беспроводной технологии согласно варианту, а нечёткому риску (RISK) присвоить значение из сформированной ранее таблицы (Рис. 5).

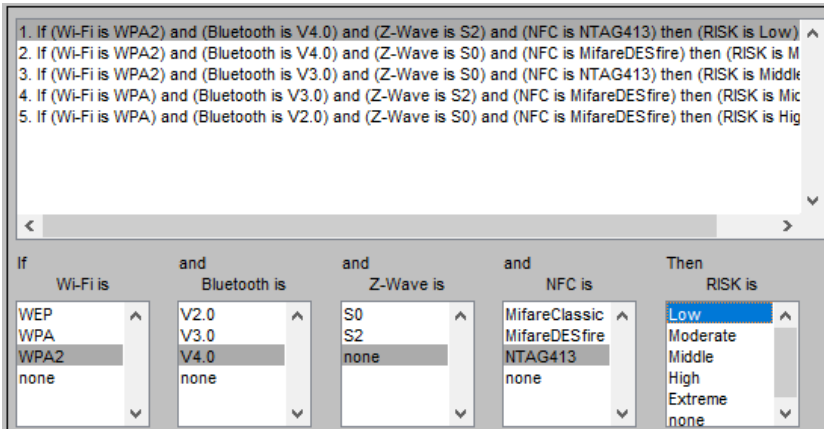

Рисунок 5 – Rule Editor.

3.4. В окне Rule Viewer (Ctrl+5 из окна Rule Editor) получить Risk для каждой комбинации протоколов и занести в отчёт. Входные значения для каждого протокола беспроводных соединений находятся в Таблице 2.

4. Получить нечёткий риск для различных версий протоколов безопасности у устройств, работающих на одной и той же беспроводной технологии.

4.1. Если в сеть добавить несколько устройств с одинаковыми типами беспроводного подключения, но разными версиями протоколов, это усложнит получение числового значения нечёткого риска с помощью инструмента Fuzzy Logic Toolbox. Теперь необходимо учитывать, что для беспроводного соединения (Wi-Fi, Bluetooth, Z-Wave, NFC согласно варианту) имеются три устройства, причем одно из них отличается версией протокола безопасности. Что бы получить верное значение нечёткого риска необходимо указать правильные входные параметры. Для всех соединений кроме тех количество которых увеличилось значение остаётся тем же.

4.2. Пример: Добавили 3 устройства работающих на технологии Wi-Fi и разных протоколах.

Таблица 4.1 – Описание имеющихся устройств.

Тип устройства	Тип подключения	Версия протокола
IP – камера	Wi-Fi	WPA2
Датчик охраны окна	Bluetooth	V4.0
Устройство охраны дома	Z-Wave	S2
NFC – считыватель	NFC	NTAG413
Датчик дыма	Wi-Fi	WPA
Блок управления отоплением	Wi-Fi	WPA

Входное значение необходимо рассчитать в соответствии с заданной функцией принадлежности (Рис. 6).

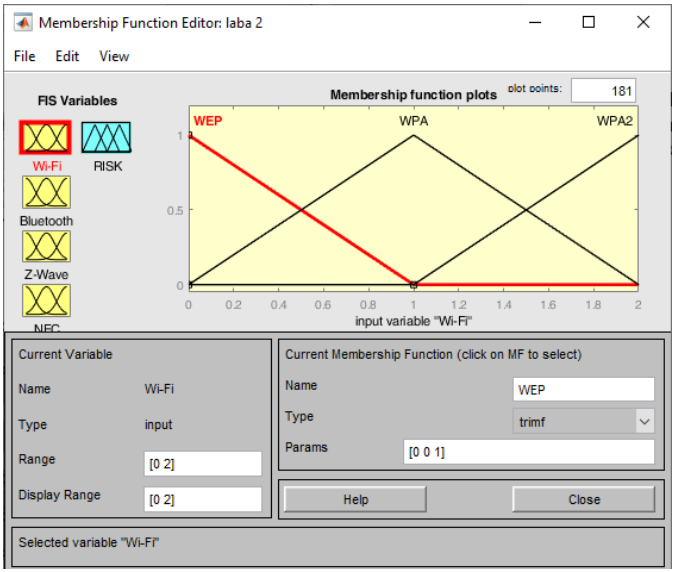

Рисунок 6 – Membership function.

Введем следующие обозначения:

b1 и b2 – значения оси абсцисс вершин функций WPA и WPA2 соответственно;

p1 и p2 – количество версий протоколов WPA и WPA2 соответственно;

x – искомое входное значение.

$$x = b1 + \frac{b2 - b1}{p1 + p2}, \quad (2)$$

$$x = 1 + \frac{2 - 1}{2 + 1}, \quad (3)$$

$$x = 1.333. \quad (3)$$

Таблица 4.2 – Определение входных значения для каждого протокола беспроводных соединений

Беспроводное соединение	Протоколы	Входное значение
Wi-FI	WPA – 2шт WPA2 – 1шт	1.333
Bluetooth	V4.0 – 1шт	2

Z-Wave	S2 – 1шт	2
NFC	NTAG413 – 1шт	2

Внеся все входные значения, указанные в таблице 4.2 в настроенный инструмент Fuzzy Logic, полученное на выходе численное значение нечеткого риска равно 0.107 (Рис.7). Значение занести в отчёт.

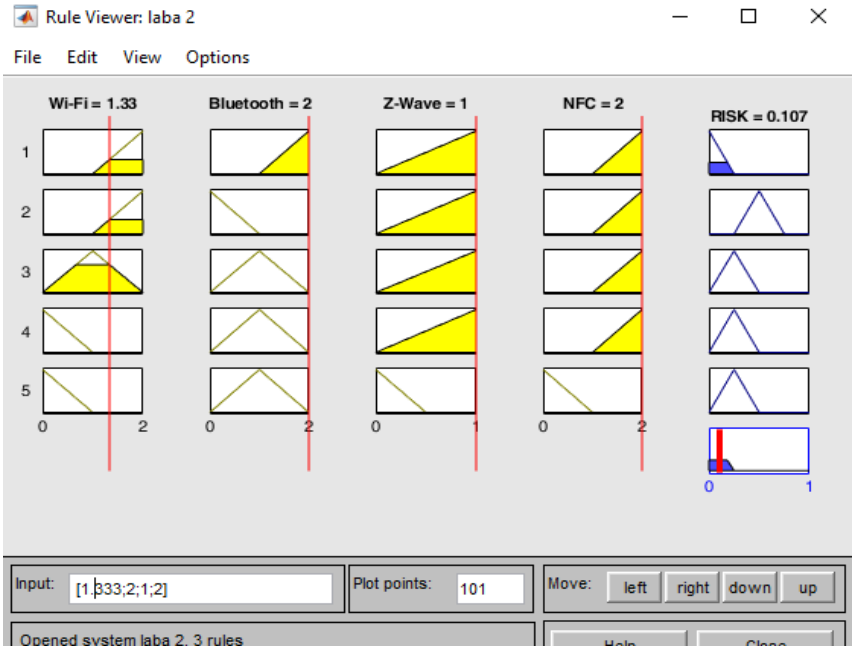

Рисунок 7 – Значение нечёткого риска.

Лабораторная работа №3
Расчет эффективности защищенности IoT-сети

Цель работы: Рассчитать эффективность использования той или иной IoT-сети с точки зрения зависимости стои-

мости этой сети от риска ее использования. Овладеть навыками моделирование сети Интернета Вещей.

Теоретические сведения

В настоящее время из-за интенсивного развития сетей построенных по технологии Интернет вещей, требуется все больше различного рода оценок и показателей этих сетей для того, чтобы будущий пользователь данной технологии имел представление об этой сети в целом. Одним из немаловажных, показателей, которые могут заинтересовать пользователя – это эффективность используемой сети.

Эффективность в данном случае подразумевает рациональность использования той или иной IoT-сети с точки зрения зависимости стоимости этой сети от риска ее использования.

Для того чтобы рассчитать эффективность выбранной IoT-сети, необходимо знать риски использования различных комбинация протоколов предполагаемой сети, стоимость устройств, которые будут использоваться, а также наличие алгоритма расчета.

В заданной IoT-сети имеется четыре устройства Интернета вещей, работающие по разным беспроводным технология. Они могут иметь различные версии протоколов безопасности. Так как известно, какое оборудование будет применяться для построения сети, необходимо найти и обозначить стоимость данного оборудования. Для удобства обозначим цены в условных единицах (таблица 5).

Таблица 5 – Таблица стоимости оборудования в зависимости от их возможностей использования различных протоколов безопасности

Используемое оборудование	Беспроводное соединение	Протоколы	Стоимость
IP-видеокамера	Wi-FI	WEP	0.4 у.е.
		WPA	0.6 у.е.

		WPA2	0.7 у.е.
Датчик охраны окна	Bluetooth	V2.0	0.1 у.е.
		V3.0	0.2 у.е.
		V4.0	0.3 у.е.
Система охраны дома	Z-Wave	S0	0.6 у.е.
		S2	1.0 у.е
Система без ключевого доступа	NFC	MifareClassic	0.8 у.е.
		MifareDESFire	0.9 у.е.
		NTAG413	1.0 у.е.

Искомое значение эффективности будет зависеть от изменения нечеткого риска различных конфигураций сети и изменения общей стоимости всего оборудования. На основании этого полученного значения, можно выбрать подходящий вариант.

Задачи

1. Изучить теоретические сведения об эффективности защищённости.
2. Получить R_{min}, R_{max}, C_{min}, C_{max}, C_1, C_2, C_3, C_4, C_5, R_1, R_2, R_3, R_4, R_5.
3. Получить отношение изменений стоимости исследуемой IoT-сети – λ.
4. Получить отношение изменений нечеткого риска исследуемой IoT-сети – σ.
5. Рассчитать эффективность – Э, для всех комбинаций протоколов.
6. Оформить отчёт по пунктам 2-5.

Порядок выполнения работы

1. Минимальный и максимальный риск и стоимость конфигурации.
   1.1. R_{min} и R_{max} – нечеткий риск минимальной и максимальной конфигурации исследуемой сети соответственно; C_{min} и C_{max} – минимальная и макси-

мальная стоимость всего оборудования сети; R_1, R_2, R_3, R_4, R_5 – нечеткий риск исследуемой сети; C_1, C_2, C_3, C_4, C_5 – стоимость всего оборудования исследуемой сети.

2. Отношение изменений стоимости исследуемой IoT-сети – λ.

$$\lambda = \frac{C_{max} - C_1}{\Delta C}, \quad (4.1)$$

где $\Delta C -$ разность максимальной и минимальной стоимости возможных комбинаций протоколов и устройств в сети:

$$\Delta C = C_{max} - C_{min}. \quad (4.2)$$

3. Отношение изменений нечеткого риска исследуемой IoT-сети – σ.

$$\sigma = \frac{R_1 - R_{min}}{\Delta R}, \quad (5.1)$$

где $\Delta R -$ разность максимального и минимального нечеткого риска возможных комбинаций протоколов и устройств в сети:

$$\Delta R = R_{max} - R_{min}. \quad (5.2)$$

4. Эффективность.

4.1. Отношение разности исходного нечеткого риска и минимально возможного нечеткого риска с разностью максимально возможного нечеткого риска исследуемой конфигурации сети и минимального значения нечеткого будут лежать в промежутке от 0 до 1.

$$0 \leq \frac{C_1 - C_{max}}{\Delta C} \leq 1, \quad (6.1)$$

$$0 \leq \frac{R_1 - R_{min}}{\Delta R} \leq 1. \quad (6.2)$$

Определив, что эффективность должна выражаться в численном значении от 0 до 1 и зная отношения изменений исходных величин сети, можно выразить

формулу для расчета значения эффективности IoT – сети, которая будет иметь вид:

$$Э = 1 - \lambda \times \sigma. \quad (6.3)$$

Полученные результаты про ранжировать и занести в отчёт.

Лабораторная работа №4
Определение Риска сети интернета вещей

Цель работы: Используя экспертные оценки для входных параметров «возможность злоумышленника», «защищенность системы», «оценка уязвимости», «оценка последствий» определить Риск для IoT – сети.

Теоретические сведения

Основной проблемой данной системы анализа риска является то, что в ней, практически на каждой стадии жизненного цикла, принимают участие эксперты. Было определено, что если изменить стандартную пару оцениваемых параметров «вероятность угрозы» и «величина ущерба», на более понятные для экспертов, то можно предположить, что экспертам будет проще их оценить, что должно сказаться на повышении достоверности конечного результата. В качестве таких параметров предложены «возможность злоумышленника», «защищенность системы», «оценка уязвимости», «оценка последствий». Необходимо определить численные параметры для каждого из логического терма всех оцениваемых параметров. То есть, задать некоторый численный интервал, например, для значения «высокий» каждой переменной. Данные численный параметры оцениваются экспертным путем с помощью опросных листов.

Следующим шагом необходимо некоторым образом агрегировать входные параметры. Очевидно, что не целесообразно подать на вход алгоритма подать все четыре и находить для них значение риска, поэтому предлагается концеп-

ция, основанная на многокаскадном применении логического интерфейса Мамдани.

В данном алгоритме оцениваются промежуточные параметры с помощью нечеткого интерфейса.

1) «Средняя возможность» = FIS1(«возможность злоумышленника»; «защищенность системы»)

2) «Средняя вероятность» = FIS2(«Средняя возможность»; «оценка уязвимости»)

3) «Риск» = FIS3(«Средняя вероятность»; «Оценка последствий»)

На рис. 8 представлена схема работы данного алгоритма, где FIS - Fuzzy Inference Model (модель нечеткого вывода)

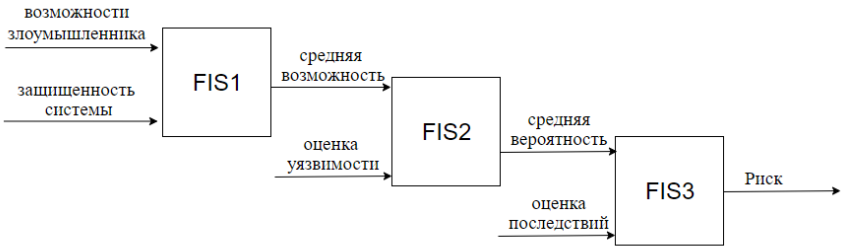

Рисунок 8 – Нечеткий алгоритм оценки риска

Задачи

1. Изучить теоретические сведения.
2. Получить выходной параметр «Средняя возможность».
3. Получить выходной параметр «Средняя вероятность»
4. Получить Риск.
5. Оформить отчёт по пунктам 2-4.

Порядок выполнения работы

1. Сперва необходимо создать первый нечеткий контроллер (Рис. 9).
   В нем указаны две входные переменные «возможности злоумышленника» - capabilities и «защищенность системы» - security и одна выходная «средняя возможность» - overallCapabilities. Каждая из данных лингвистических переменных имеет свой набор функций принадлежности, которые все описывают значения «низкий» (0-0,3), «средний» (0,3-0,7), «высокий» (0,7-1) (Рис. 10-11).

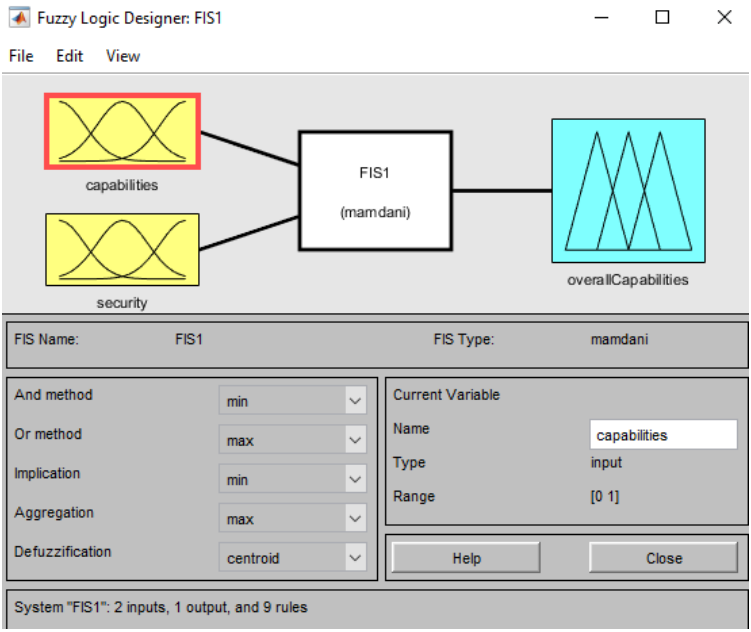

Рисунок 9 – Окно создания первого нечеткого интерфейса

Для переменной capabilities функции принадлежности low – [-0.1 0.15 0.3], medium – [0.3 0.5 0.7], high – [0.7 0.85 1.1].

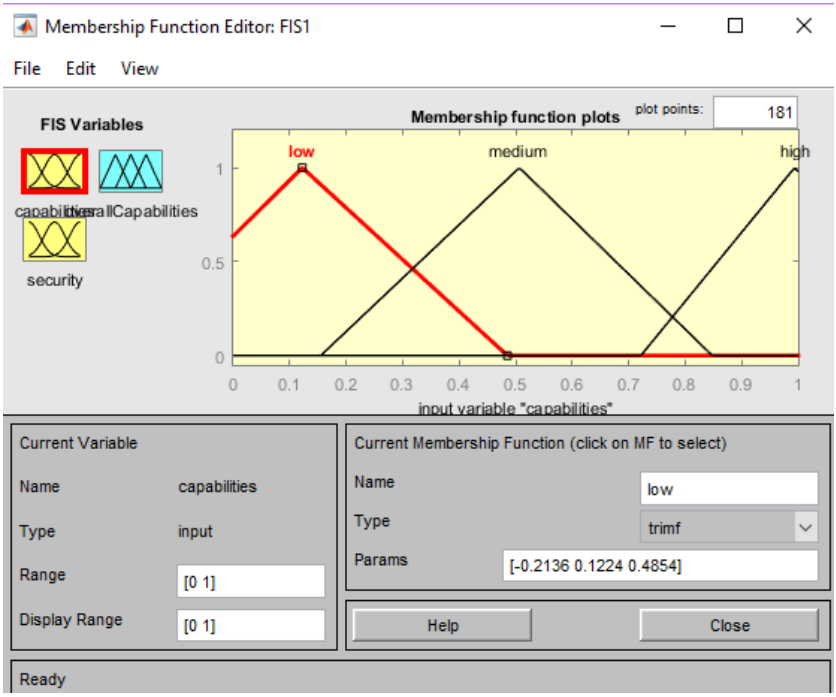

Рисунок 10 – Функции принадлежности переменной «возможность злоумышленника»

Для переменной security функции принадлежности low – [-0.1 0 0.3], medium – [0.2 0.5 0.8], high – [0.7 1 1.1].

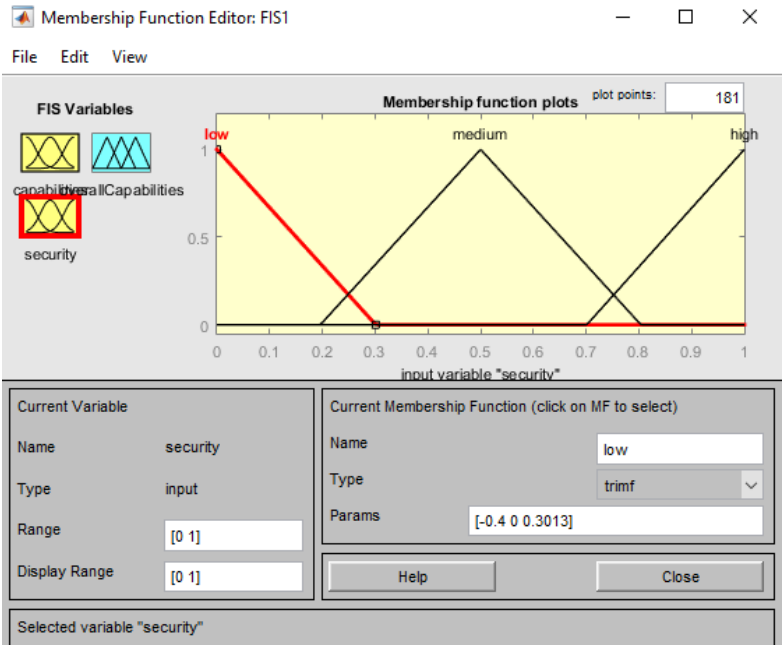

Рисунок 11 – Функции принадлежности переменной «защищенность системы»

1.1. Создание решающих правил.

Необходимо задать логические правила. Правила формируются в соответствии с таблицей, на пересечении – значение overallCapabilities (таблица 6):

Таблица 6 – Правила для FIS1

		capabilities		
		низкий	средний	высокий
security	низкий	низкий	средний	высокий
	средний	низкий	низкий	средний
	высокий	низкий	низкий	средний

В соответствии с этой таблицей, задаем нечеткие правила (рис. 12).

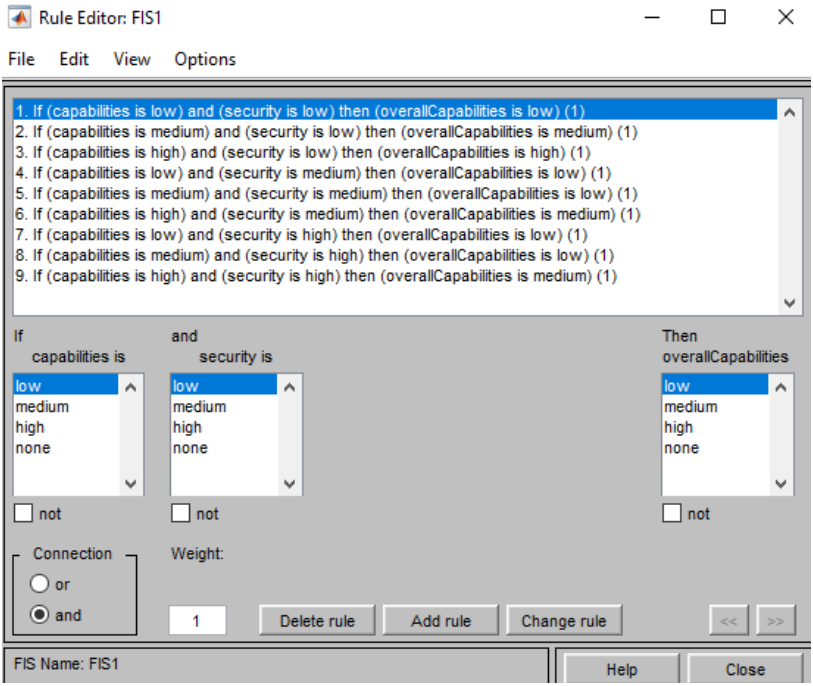

Рисунок 12 – Набор правил для FIS1

Выходная переменная первого интерфейса является входной переменной для второго, помимо этого добавляется новая переменная – оценка уязвимости.

2. Зададим входные и выходные переменные для FIS2 (рис. 13).

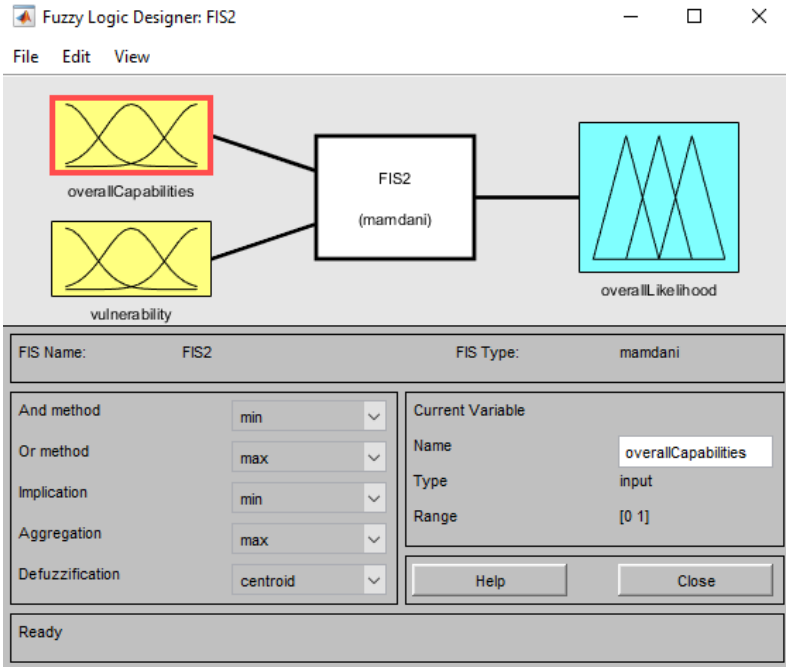

Рисунок 13 – Второй нечеткий интерфейс

Для переменной overallCapabilities функции принадлежности low – [-0.4 0 0.4], medium – [0.103 0.503 0.903], high – [0.6 1 1.4] (Рис.14).

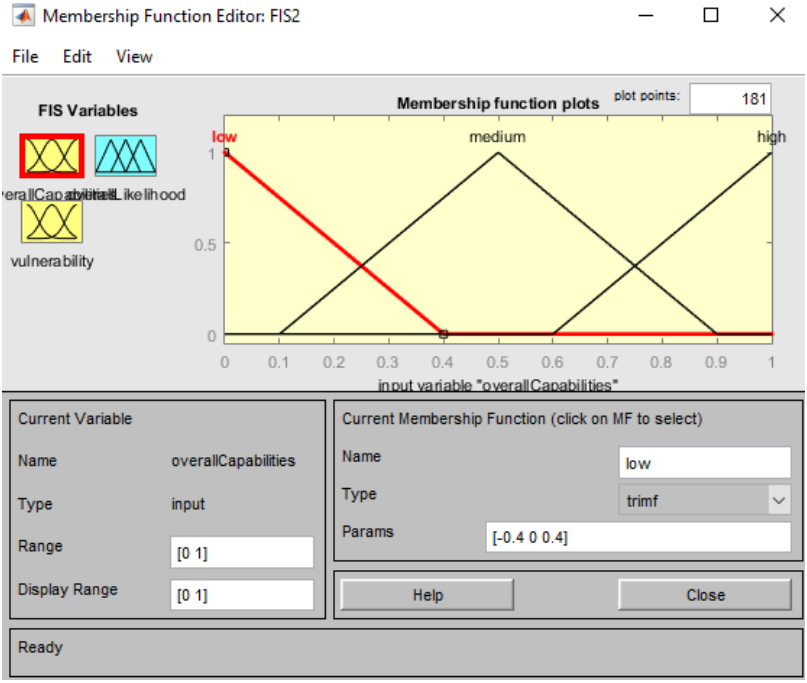

Рисунок 14 – Функции принадлежности входной переменной «средняя возможность»

Для переменной vulnerability функции принадлежности low – [-0.405 0 0.3], medium – [0.2 0.45 0.7], high – [0.6 1 1] (Рис.15).

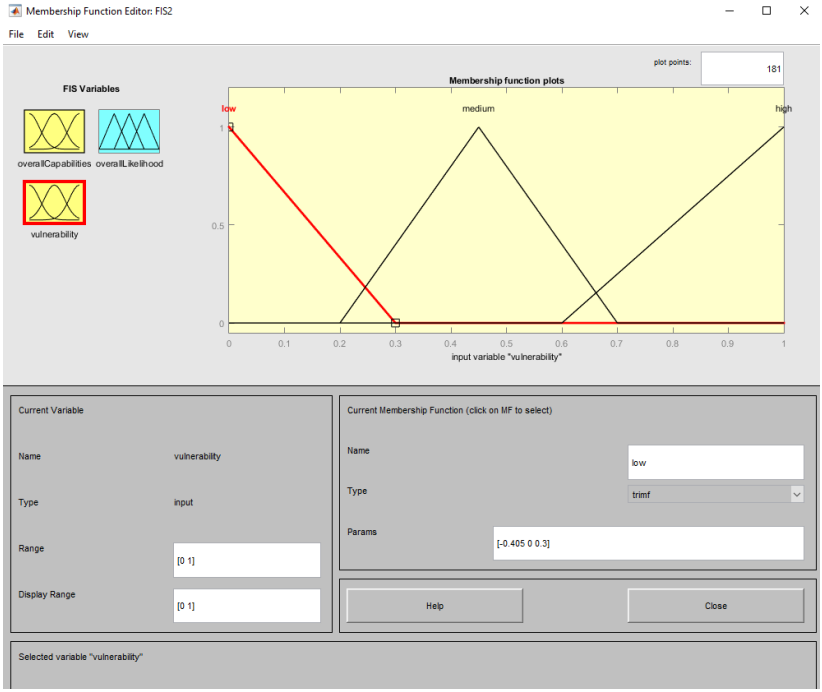

Рисунок 15 – Функции принадлежности переменной «оценка уязвимости»

Для переменной overallLikelihood функции принадлежности low – [-0.4 0 0.4], medium – [0.1 0.5 0.9], high – [0.7 1 1.4] (Рис.16).

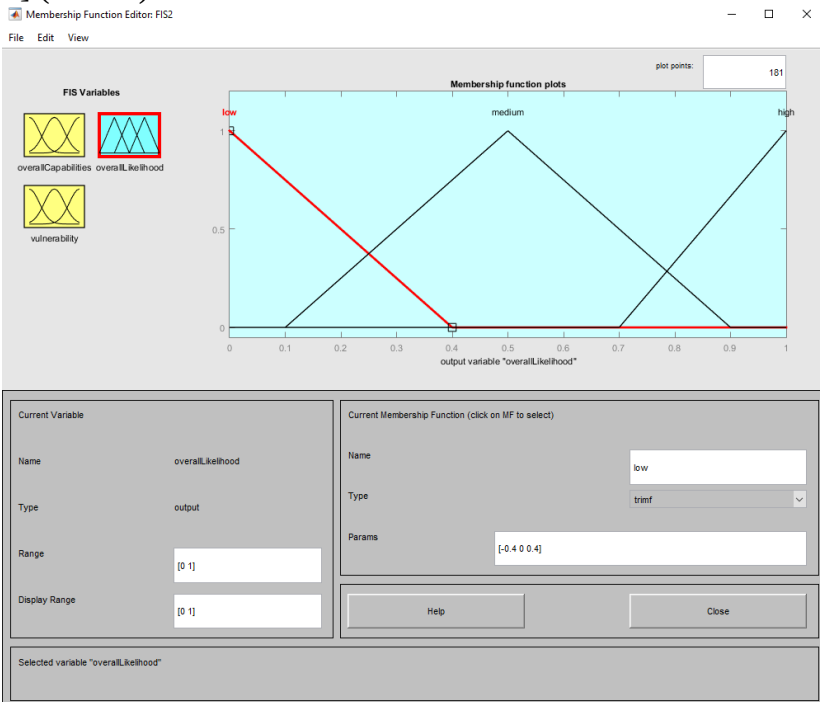

Рисунок 16 – Функции принадлежности выходной переменной «средняя вероятность»

2.1. Создание решающих правил.

Для второго интерфейса также необходимо задать логические правила (Рис.17). Правила формируются в соответствии с матрицей, на пересечении – значение overallLikelihood (таблица 7). Т.е. чем выше один из параметров, тем выше и значение на пересечении:

Таблица 7 – Правила для FIS2

		overallCapabilities		
		низкий	средний	высокий
vulnerability	низкий	низкий	средний	высокий
	средний	средний	средний	высокий
	высокий	средний	высокий	высокий

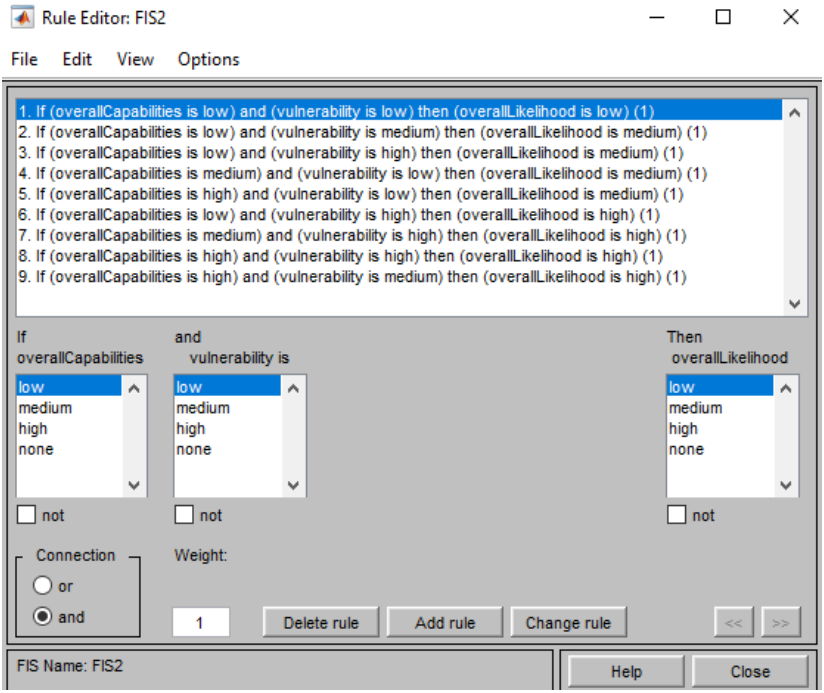

Рисунок 17 – Набор правил FIS2

Выходной параметр overallLikelihood является входным параметром для третьего нечёткого интерфейса.

3. Третий нечеткий интерфейс с дополнительным параметром «оценка последствий» (Рис.18).

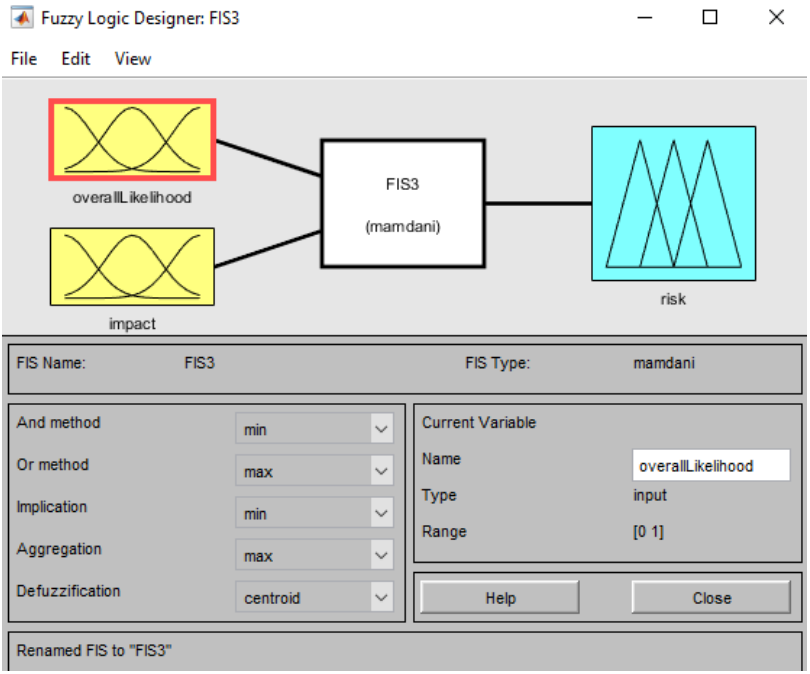

Рисунок 18 – Третий нечеткий интерфейс

Зададим функции принадлежности для переменных «средняя вероятность» (Рис.19), «оценка последствий» (Рис.20), и выходной переменной «риск» (Рис.21).

Для переменной overallLikelihood функции принадлежности low – [-0.4 0 0.4], medium – [0.1 0.5 0.9], high – [0.7 1 1.4] (Рис.19).

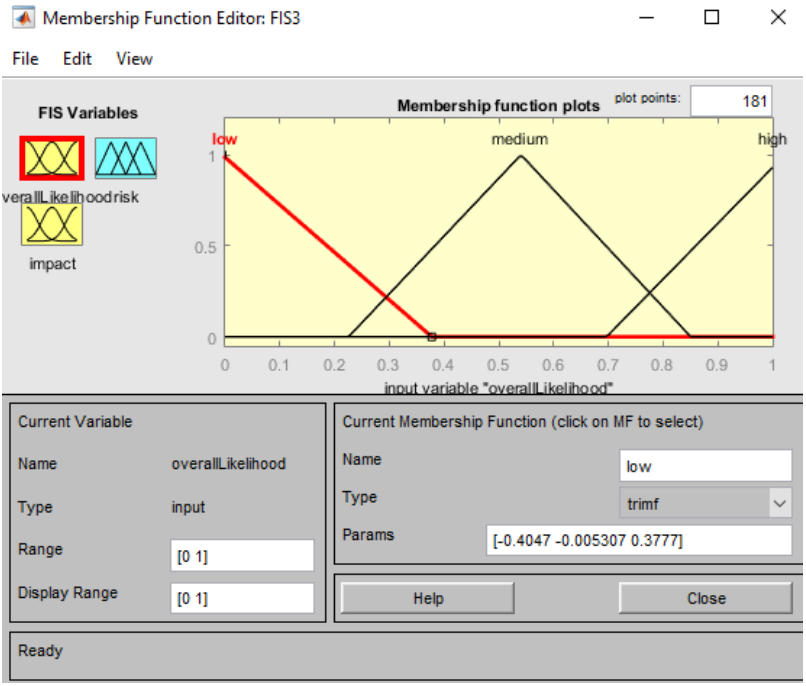

Рисунок 19 - Функции принадлежности входной переменной «средняя вероятность»

Для переменной impact функции принадлежности low – [0 0 0.4], medium – [0.2 0.5 0.8], high – [0.7 1 1.4] (Рис.20).

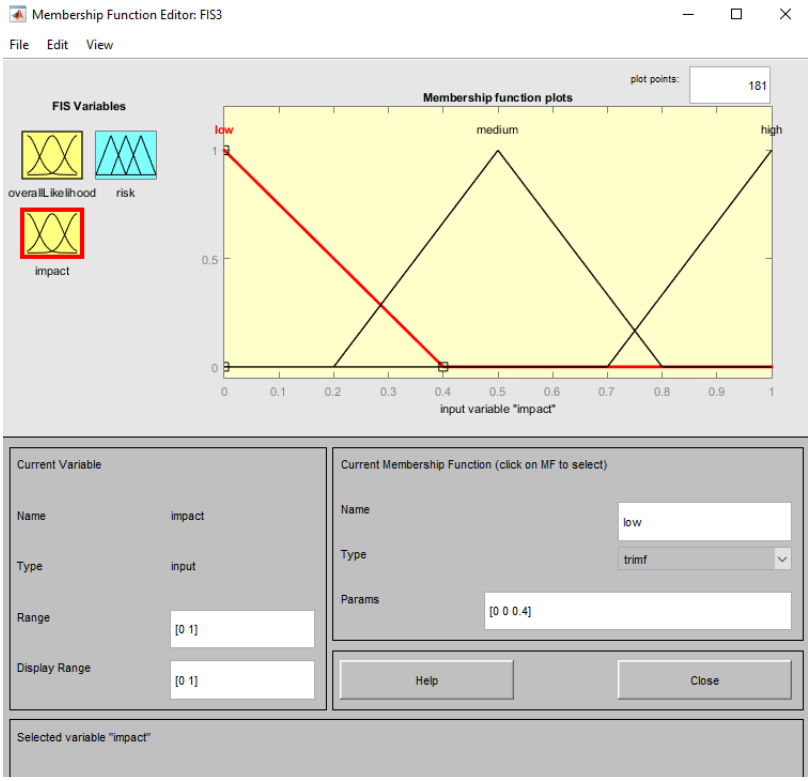

Рисунок 20 - Функции принадлежности переменной «оценка последствий»

Для переменной risk функции принадлежности low – [-0.2 0 0.3], medium – [0.1 0.5 0.8], high – [0.55 0.97 1.4] (Рис.21).

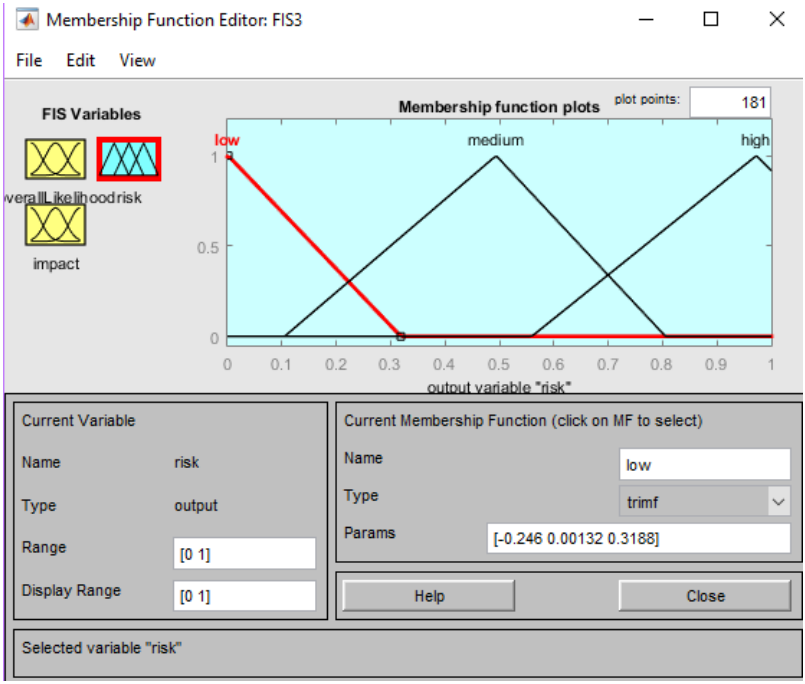

Рисунок 21 – Функции принадлежности «риск»

Аналогично, как и для предыдущих интерфейсов формируем правила (Рис.22) для FIS3 (таблица 8). На пересечении – значение риска.

Таблица 8 – Правила для FIS3

		overallLikelihood		
		низкий	средний	высокий
impact	низкий	низкий	средний	средний
	средний	средний	средний	высокий
	высокий	средний	высокий	высокий

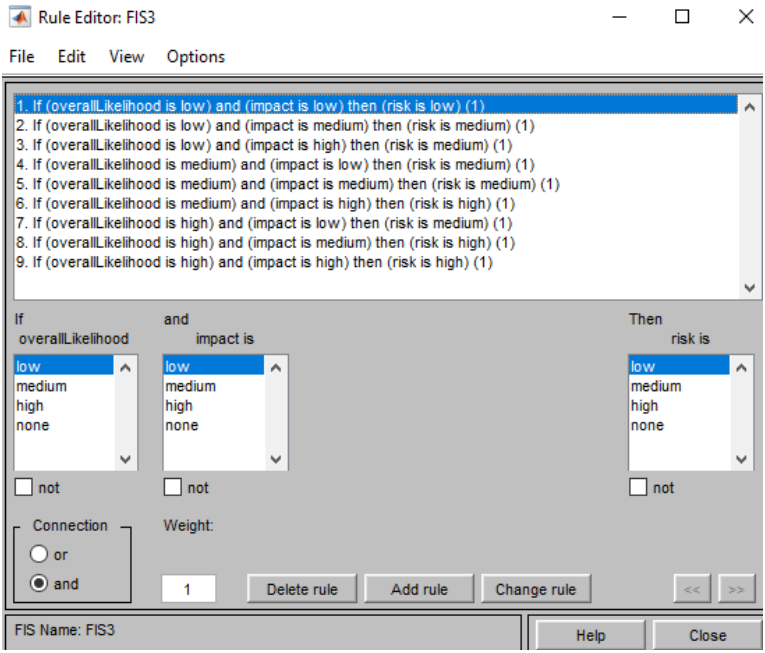

Рисунок 22 - Набор правил FIS3

Подставив экспертные оценки для входных переменных «возможность злоумышленника», «защищенность системы», «оценка уязвимости», «оценка последствий» согласно варианту, получить риск для сети интернета вещей.

Например, экспертами были оценены параметры:

1) Capability = 0.658;
2) Security = 0.636;
3) Vulnerability = 0.268;
4) Impact = 0.446.

По результатам выполнения программы, получаем промежуточные значения для overallCapability = 0.149 (Рис.23), overallLikelihood = 0.47 (Рис.24). И в результате получаем риск (risk) равный 0.467 (Рис.25).

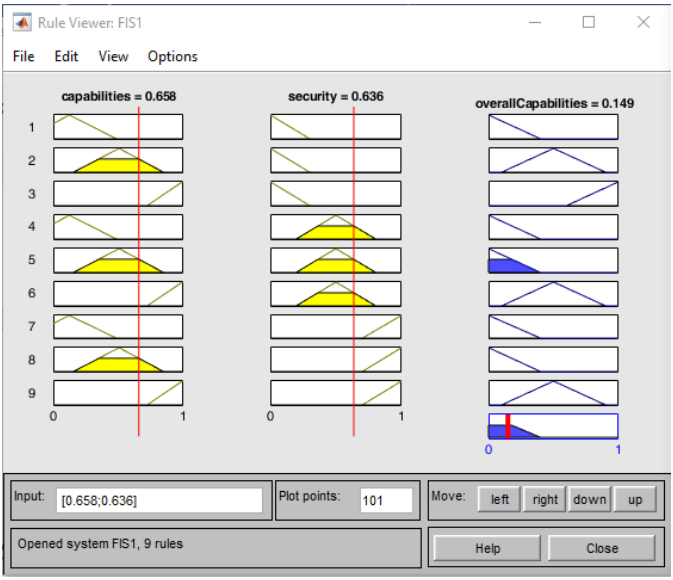

Рисунок 23 – Первый нечеткий интерфейс

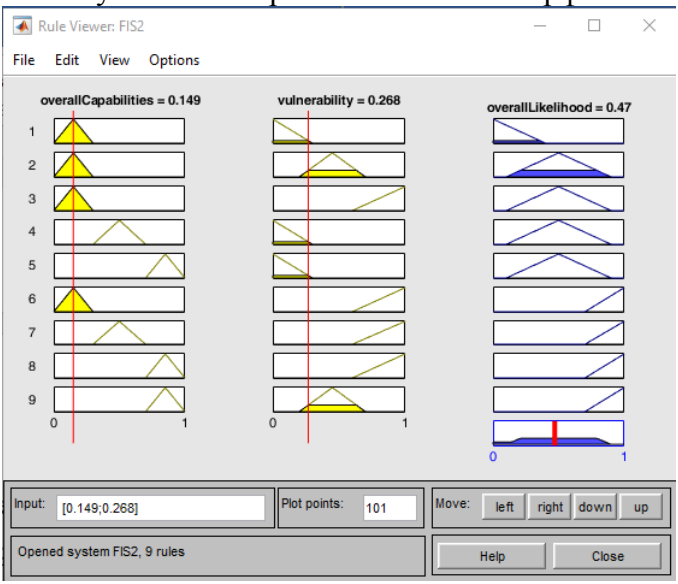

Рисунок 24 – Второй нечеткий интерфейс

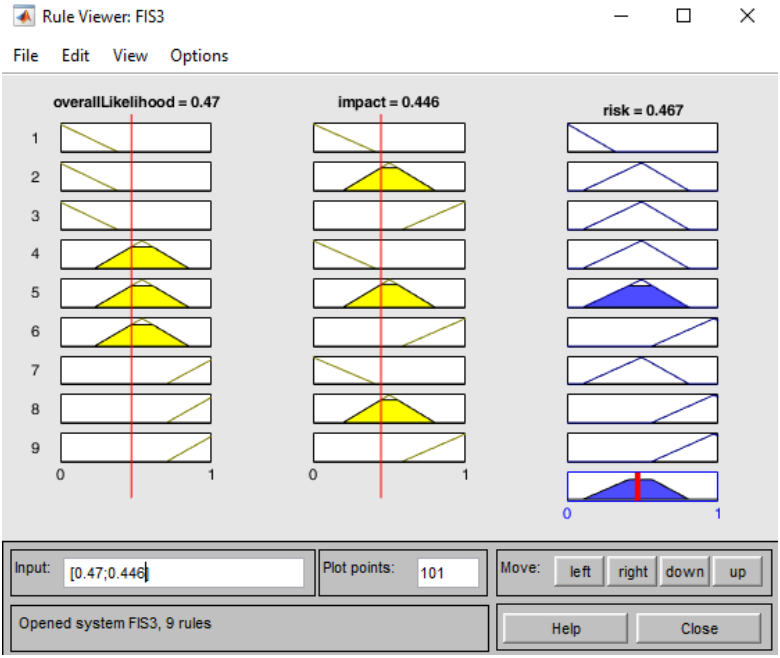

Рисунок 25 – Третий нечеткий интерфейс

Полученное значение риска занести в отчёт.

Лабораторная работа №5
Автоматизированное нахождение решающих правил для нечёткого логического интерфейса

Цель работы: получить количество продукционных правил для N атак. С помощью, языков программирования написать алгоритм для составления решающих правил, сделать выводы о влиянии количества решающих правил на конечный результат ущерба беспроводной сети. Выработать рекомендации к построению эффективной сети интернета вещей.

Теоретические сведения

1. Типы атак, воздействующих на беспроводную IoT – сеть. Атаки на беспроводные локальные сети направлены на конфиденциальность и целостность информации, а также на доступность сети. Данные атаки безопасности могут быть пассивными или активными.

Пассивная атака состоит из несанкционированного доступа к ресурсу или сети с целью прослушивания или анализа трафика, но не для изменения его содержимого. Ее достаточно сложно обнаружить, потому что в процессе ее реализации данные остаются неизменными.

Активная атака состоит из несанкционированного доступа к ресурсу или сети с целью внесения изменений в сообщение, поток данных или файл, или с целью нарушения работы сетевой службы [4-5].

В данной лабораторной работе будут рассмотрены следующие атаки на сеть:

1) Атака с помехами (Jamming attack) – передача информации на той частоте, на которой находится целевая WLAN, возможно, при мощности, превышающей норматив эквивалентной изотопно-излучаемой мощности (EIRP).

2) Атака клонов (Clone attack) – в этой атаке атакующий копирует узлы в форме клона.

3) Атака манипулирования информацией о маршруте (Route information manipulation attack) – в этой атаке злоумышленник дает ложную информацию о маршрутизации.

4) Атака отказа в обслуживании (Denial of service attack) - происходит из-за сбоя узла или вредоносного действия.

5) Атака подслушивающего устройства (Eavesdropping attack) – захват и декодирование незащищенного трафика приложений для получения потенциально конфиденциальной информации.

6) Атака столкновения (Collision attack) – создает прерывание в работающей беспроводной сети.

7) Атака провала (Sink hole attack) – в случае реализации атаки провала существует серьезная угроза того, что

скомпрометированный узел пытается получить весь или значительный трафик из определенной области.

8) Атака анализа трафика (Traffic analysis attack) – это тип атаки на безопасность сети, который создает трафик в беспроводной сети.

9) Атака десинхронизации (De-synchronization attack) – десинхронизация изменяет порядковый номер пакета.

10) Атака с избирательной переадресацией (Selective forwarding attack) – в этой атаке скомпрометированный узел отбрасывает пакеты, которые влияют на эффективность сети [6].

Задачи

1. Изучить теоретические сведения о типах атак на беспроводные сети.
2. Описать входные и выходные переменные для алгоритма Мамдани для нахождения ущерба.
3. Рассчитать количество решающих правил для N атак.
4. С помощью любого языка программирования перебрать все варианты решающих правил для N атака.
5. Внести полученные правила в файл FIS и проверить их корректность.
6. Сделать выводы о влиянии количества корректно описанных правил на конечный численный результат на выходе нечеткой системы.
7. Оформить отчёт по пунктам 2-6.

Порядок выполнения работы

1. Входные и выходные параметры.
   1.1. В лабораторной работе от 5 до 10 входных параметров в зависимости от варианта:
   1) Атака отказа в обслуживании (Denial of service attack);

2) Атака подслушивающего устройства (Eavesdropping attack);
3) Атака столкновения (Collision attack);
4) Атака провала (Sink hole attack);
5) Атака анализа трафика (Traffic analysis attack);
6) Атака десинхронизации (De-synchronization attack);
7) Атака с избирательной переадресацией (Selective forwarding attack);
8) Атака с помехами (Jamming attack);
9) Атака клонов (Clone attack);
10) Атака манипулирования информацией о маршруте (Route information manipulation attack).

Для каждого из входных параметров необходимо указать терм-множество в зависимости от влияния или его отсутствия конкретной атаки на беспроводную сеть: «нет» и «да». Кроме того, будет один выходной параметр с именем ISAN (Impact of Security Attack on Network – Влияние атаки на безопасность сети), определяющий значение ущерба беспроводной сети (Рис.26).

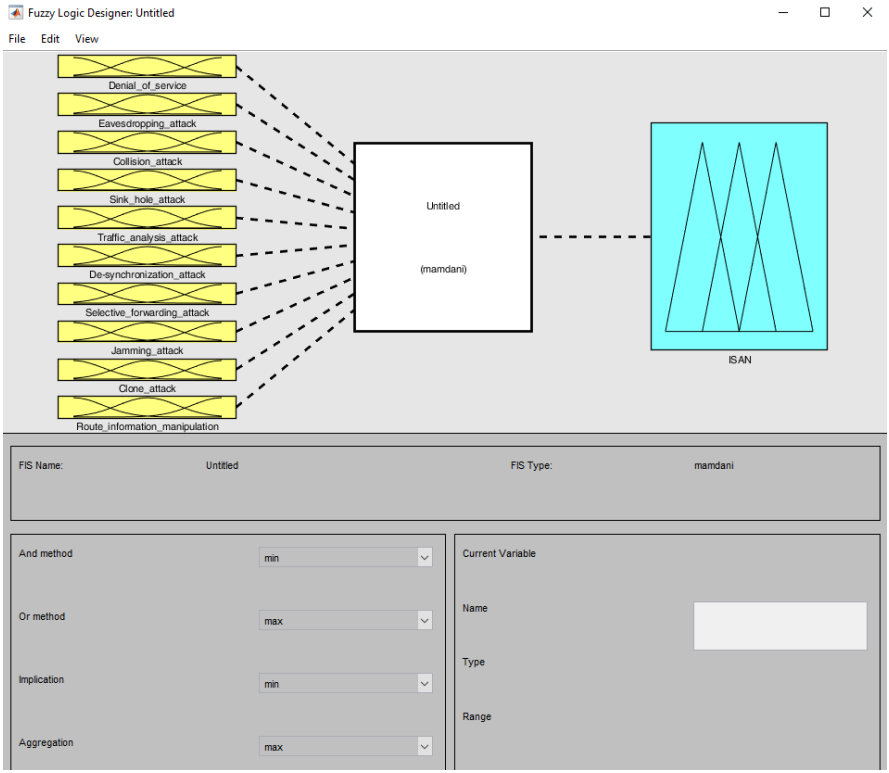

Рисунок 26 – Выходные и выходные параметры.

Функции принадлежности входных параметров. Функции принадлежности назвать нет (no): Type – trimf, Params [0 0.001 0.61] и да(yes): Type – trimf, Params [0.39 0.999 1.1]. Для всех входных параметров установить аналогичные настройки.

Функция принадлежности выходной переменной. В данной работе будет использоваться 5 термножеств для лингвистической переменной оценки ущерба ISAN, предназначенных для описания уровня воздействия на сеть: очень низкий, низкий, средний, высокий, очень высокий.

2. Формула для расчёта всех возможных вариантов комбинаций решающих правил (1):

$$C_m^0 + C_m^1 + C_m^2 + C_m^3 + \cdots + C_m^n = K, \quad (1)$$

где n = m, m = количество атак, направленных на беспроводную сеть.

Для расчёта комбинаций использовать формулу (2):

$$C_m^n = \frac{m!}{n!(m-n)!}, \quad (2)$$

Где m = количество атак,

n = атаки используемые в комбинации.

3. Написание алгоритма перебора всех возможных вариантов решающих правил. Для этого открыть файл FIS созданный в первом пункте, в любом текстовом редакторе (Рис.27).

```
[Rules]
2 1 2 1 2 1 1 2 1 2, 4 (1) : 1
2 2 2 1 1 1 2 1 1 2, 5 (1) : 1
2 2 2 1 2 2 1 1 1 1, 3 (1) : 1
2 2 2 2 2 2 2 1 2 2, 5 (1) : 1
1 2 1 1 1 1 1 1 1 1, 1 (1) : 1
2 1 2 1 1 1 1 1 1 1, 2 (1) : 1
```

Рисунок 27 – Продукционные правила

После строчки [Rules] следуют правила, каждая строчка означает набор правил, каждое число в строке означает функцию принадлежности 1 – нет, 2 – да, порядок числа соответствует порядку переменных (атак) объявленных в первом пункте, число после запятой – выходная переменная Ущерб IoT – сети: 1 – Очень низкий (VL), 2 – Низкий (L), 3 – Средний (M), 4 – Высокий (H), 5 – Очень высокий (VH). Продолжение строки оставить неизменным. Полученные продукционные правила, поместить в файл FIS, запустить и проверить их корректность, результаты лабораторной работы занести в отчёт.

Приложение А. Варианты для лабораторных работ 1-5

Номер варианта	Набор протоколов беспроводных соединений в сети 1-3 Л.Р.
0	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and NTAG413 2. WPA2 and V2.0 and S2 and NTAG413 3. WPA and V3.0 and S2 and NTAG413 4. WEP and V3.0 and S2 and NTAG413 5. WEP and V3.0 and S0 and MifareClassic 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: WPA – 2шт,WPA2 – 1шт
1	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and NTAG413 2. WPA2 and V4.0 and S0 and MifareDESFire 3. WPA2 and V3.0 and S0 and NTAG413 4. WPA and V3.0 and S2 and MifareClassic 5. WPA and V2.0 and S0 and MifareDESFire 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: WEP – 2шт,WPA2 – 1шт
2	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and MifareDESFire 2. WPA2 and V4.0 and S0 and MifareClassic 3. WPA2 and V3.0 and S0 and MifareDESFire 4. WPA and V3.0 and S0 and NTAG413 5. WPA and V2.0 and S0 and MifareClassic 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: WEP – 2шт,WPA – 1шт
3	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and NTAG413

	1-2 Лабораторная работа. 2. WPA2 and V3.0 and S2 and MifareDESFire 3. WPA2 and V3.0 and S0 and MifareClassic 4. WPA and V3.0 and S0 and MifareDESFire 5. WEP and V4.0 and S0 and MifareClassic 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: V3.0 – 2шт,V4.0 – 1шт
4	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S0 and NTAG413 2. WPA2 and V3.0 and S2 and MifareClassic 3. WPA2 and V2.0 and S2 and MifareDESFire 4. WPA and V3.0 and S0 and MifareClassic 5. WEP and V3.0 and S0 and MifareDESFire 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: V4.0 – 2шт,V3.0 – 1шт
5	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and MifareClassic 2. WPA2 and V2.0 and S2 and NTAG413 3. WPA2 and V2.0 and S2 and MifareClassic 4. WPA and V2.0 and S2 and MifareDESFire 5. WEP and V2.0 and S2 and MifareDESFire 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: V2.0 – 2шт,V3.0 – 1шт
6	1-2 Лабораторная работа. 1. WPA2 and V3.0 and S2 and NTAG413 2. WPA and V4.0 and S2 and NTAG413 3. WPA2 and V2.0 and S0 and NTAG413 4. WPA and V2.0 and S2 and MifareClassic 5. WEP and V2.0 and S2 and MifareClassic 3 Лабораторная работа.

	Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами без опасности: S0 – 2шт,S2 – 1шт
7	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S0 and NTAG413 2. WPA and V4.0 and S2 and MifareDESFire 3. WPA2 and V2.0 and S0 and MifareDESFire 4. WPA and V2.0 and S0 and NTAG413 5. WEP and V2.0 and S2 and MifareClassic 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: S2 – 2шт,S0 – 1шт
8	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and MifareClassic 2. WPA and V4.0 and S2 and MifareClassic 3. WPA2 and V2.0 and S0 and MifareClassic 4. WEP and V4.0 and S2 and NTAG413 5. WEP and V2.0 and S2 and MifareClassic 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: MifareClassic – 2шт, MifareDESFire – 1шт
9	1-2 Лабораторная работа. 1. WPA2 and V3.0 and S2 and NTAG413 2. WPA and V4.0 and S2 and MifareClassic 3. WPA2 and V2.0 and S0 and MifareClassic 4. WEP and V4.0 and S2 and NTAG413 5. WEP and V2.0 and S0 and NTAG413 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: MifareDESFire – 2шт, MifareClassic – 1шт
10	1-2 Лабораторная работа. 1. WPA2 and V4.0 and S2 and MifareDESFire

	2. WPA2 and V2.0 and S2 and NTAG413 3. WPA and V4.0 and S0 and MifareDESFire 4. WEP and V4.0 and S2 and MifareDESFire 5. WEP and V2.0 and S0 and MifareDESFire 3 Лабораторная работа. Протоколы для проверки алгоритма расчёта нечёткого риска при наличии нескольких видов беспроводного подключения с разными протоколами безопасности: NTAG413 – 2шт, MifareDESFire – 1шт

Номер варианта	Входные параметры
1	4 лабораторная работа: 1) Capability = 0.628; 2) Security = 0.601; 3) Vulnerability = 0.311; 4) Impact = 0.464. 5 лабораторная работа: **5 реализуемых атак.**
2	4 лабораторная работа: 1) Capability = 0.701; 2) Security = 0.728; 3) Vulnerability = 0.212; 4) Impact = 0.399. 5 лабораторная работа: **6 реализуемых атак.**
3	4 лабораторная работа: 1) Capability = 0.833; 2) Security = 0.547; 3) Vulnerability = 0.425; 4) Impact = 0.627. 5 лабораторная работа: **7 реализуемых атак.**
4	4 лабораторная работа: 1) Capability = 0.899; 2) Security = 0.572; 3) Vulnerability = 0.395; 4) Impact = 0.592. 5 лабораторная работа: **8 реализуемых атак.**
5	4 лабораторная работа: 1) Capability = 0.905; 2) Security = 0.757; 3) Vulnerability = 0.245; 4) Impact = 0.666. 5 лабораторная работа: **9 реализуемых атак.**
6	4 лабораторная работа: 1) Capability = 0.550;

	2) Security = 0.825; 3) Vulnerability = 0.296; 4) Impact = 0.229. 5 лабораторная работа: **10 реализуемых атак.**
7	4 лабораторная работа: 1) Capability = 0.499; 2) Security = 0.645; 3) Vulnerability = 0.258; 4) Impact = 0.385. 5 лабораторная работа: **9 реализуемых атак.**
8	4 лабораторная работа: 1) Capability = 0.493; 2) Security = 0.712; 3) Vulnerability = 0.232; 4) Impact = 0.326. 5 лабораторная работа: **8 реализуемых атак.**
9	4 лабораторная работа: 1) Capability = 0.385; 2) Security = 0.699; 3) Vulnerability = 0.260; 4) Impact = 0.296. 5 лабораторная работа: **7 реализуемых атак.**
10	4 лабораторная работа: 1) Capability = 0.468; 2) Security = 0.340; 3) Vulnerability = 0.632; 4) Impact = 0.554. 5 лабораторная работа: **6 реализуемых атак.**

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кучерявый, А. Е. Интернет Вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21-24.

2. Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире // Мобильные телекоммуникации. – 2016. – №10. – С. 20-26.

3. T. A. Alghamdi, A. Lasebae, and M. Aiash, «Security analysis of the constrained application protocol in the internet of things» in Future Generation Communication Technology (FGCT), 2015 Second International Conference on. IEEE, 2013, pp. 163-168.

4. Asosheh A. A new quantitative approach for information security risk assessment / A. Asosheh, B. Dehmoubed, A. Khani. – IEEE Intelligence and Security Informatics Conference, Richardson, Dallas, TX, USA, 2009.

5. Bernardo D. V. Quantitative Security Risk Assessment (SRA) Method: An empirical case study / D. V. Bernardo B. B. Chua D. Hoang. – World Congress on Nature amp; Biologically Inspired Computing, Coimbatore, India, 2009. – PP. 972 – 977.

6. Skorupski J. The simulation-fuzzy method of assessing the risk of air traffic accidents using the fuzzy risk matrix / J. Skorupski. – Safety Science 88, 2016. – PP. 76 – 87.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Безопасность информационных систем и сетей интернета вещей»
для студентов специальности 10.05.03 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составитель
Ермаков Сергей Александрович

В авторской редакции

Подписано к изданию __.04.2021.
Уч.-изд. л. __

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14