МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, к.э.н. |  |  |  | Т.Н. Елина |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №3 | | | | |
| АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОМ НЕЧЕТКОЙ ЛОГИКИ | | | | |
| по курсу: МЕТОДОЛИГИЯ ЗАЩИТЫ ИНФОРМАЦИИ | | | | |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | 3843 |  |  |  | Калинина А.С,  Конева А.П., Шумков Е.Г. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2021

1. **Цель работы**: провести анализ уровней реализации методов защиты и оценить защищенность организации с точки зрения конкретного показателя (комплекса показателей).
2. **Задачи**: провести системный анализ выбранной предметной области (организации). На основании полученных данных выделить направления защиты, оценить уровни их реализации. Разработать систему нечетких правил. Охарактеризовать показатель (комплекс показателей) с точки зрения защищенности.

В рамках выполняемой лабораторной работы рассматривается деятельность нотариальной конторы.

Нечетка логика – это набор нестрогих правил, в которых для достижения поставленной цели могут использоваться радикальные идеи, интуитивные догадки, а также опыт специалистов, накопленный в соответствующей области.

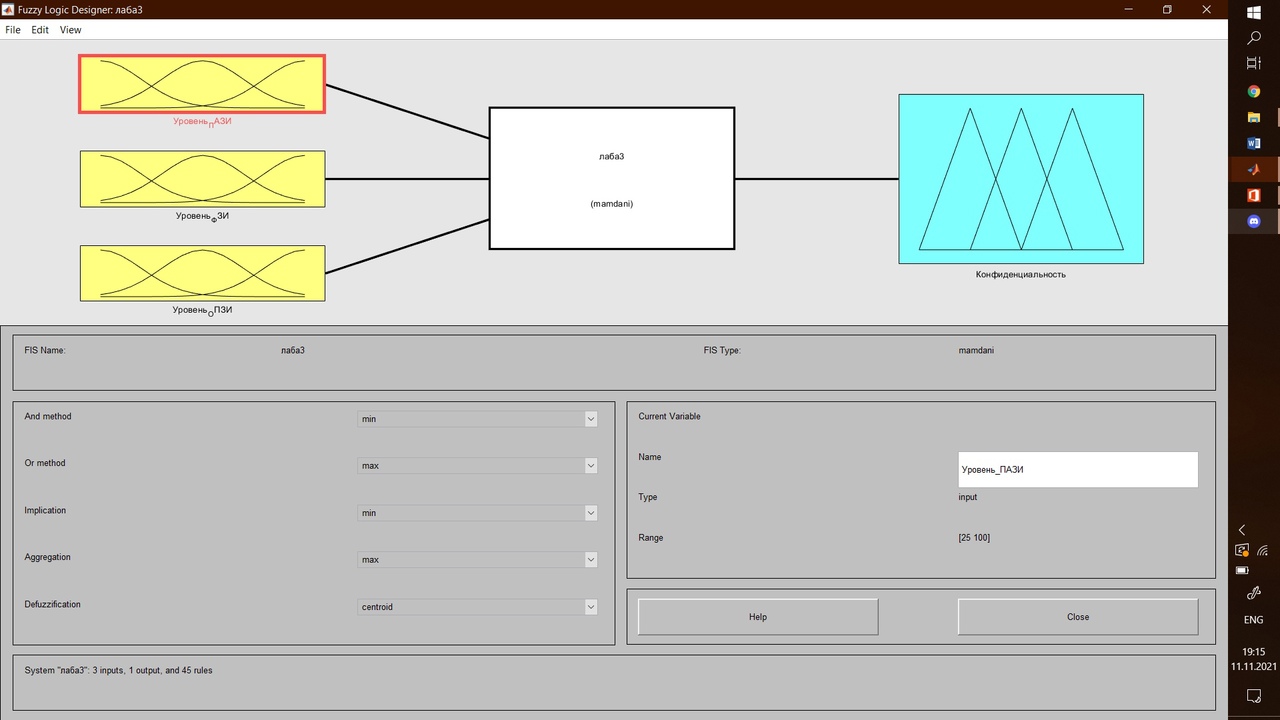
Для описания нечетких множеств, представляющих собой входные и выходные переменные, используются нечеткие и лингвистические переменные. Нечеткая переменная – это терм, который описывается набором, состоящим из названия переменной, ее области определения, а также набором возможных значений. Обобщением нечеткой переменной является лингвистическая переменная, значениями такой переменной могут быть термы. На рисунке 1 представлена структура и взаимосвязь переменных.

Рисунок 1 – Структура системы

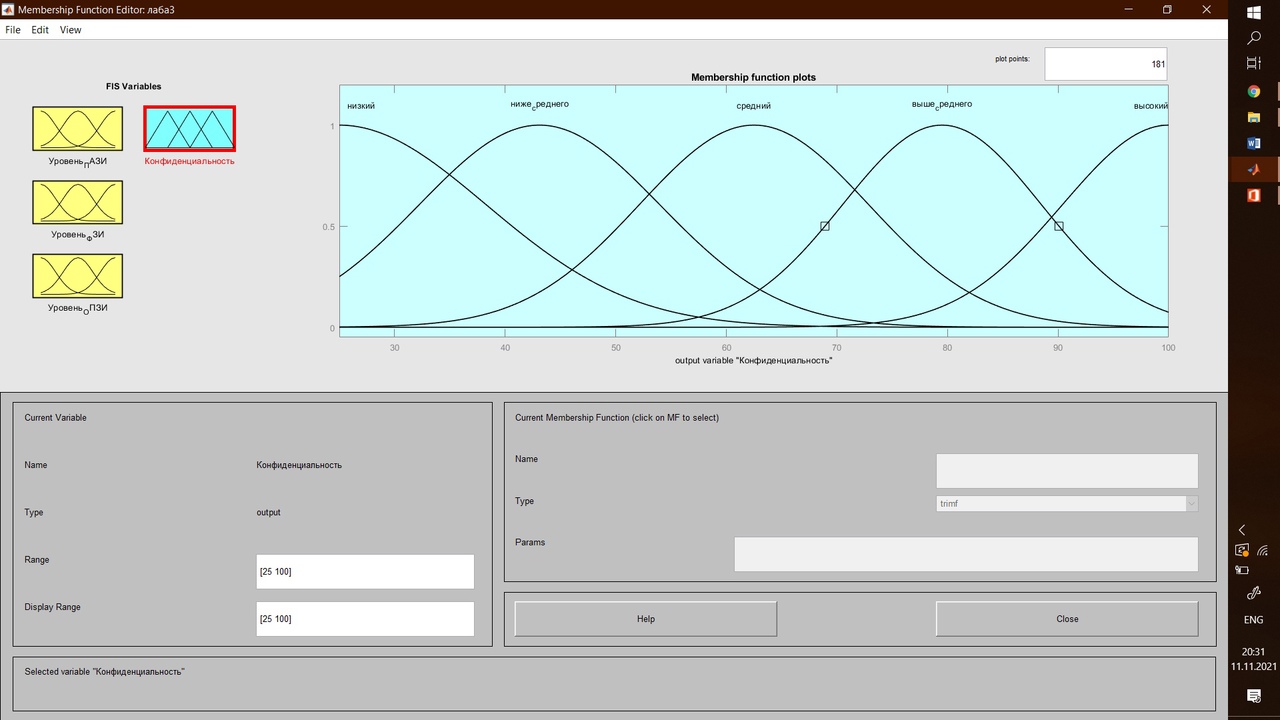
В качестве выходной переменной оценивается риск нарушения конфиденциальности данных. Для нее были выделены следующие термы: низкий, ниже среднего, средний, выше среднего, высокий. Данная переменная представлена на рисунке 2.

Рисунок 2 – Выходная переменная

В рамах данной лабораторной работы были выделены три входные лингвистические переменные:

* + - 1. Уровень программно – аппаратной защиты, включающий в себя использование различных электронных устройств и специальных программ. Сюда можно отнести следующие методы защиты:

1. Аутентификация по SSH для доступа к серверу;
2. Периодическое создание бэкапа данных;
3. Аудит файлов с помощью IDS/IPC;
4. Использование антивирусного ПО и файрвола;
5. Использование программного средства защиты информации от несанкционированного доступа;
6. Печать с автоматической маркировкой каждой страницы;
7. Использование системы Screen Guard;
8. Отключение портов ПК для предотвращения использование внешних носителей.
   * + 1. Уровень физической защиты, методы которого основаны на применении разного рода механических, электро – и электронно - механических устройств и сооружений, предназначенных для создания физических препятствий на возможных путях проникновений и доступа потенциальных нарушителей к компонентам системы и защищаемой информации. К данным методам относятся:
          1. Доступ в помещение по ID – карте и установка охранной сигнализации;
          2. Установка механических замков на дверцы шкафчиков с документацией и использование защитной пленки на окнах;
          3. Установка системы видеонаблюдения и пожарной сигнализации.
       2. Уровень организационно – правовой защиты, включающий в себя меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использования ее ресурсов, а также деятельность сотрудников организации. К мерам защиты относятся:
9. Инструктаж сотрудников организации и заключение соглашений о неразглашении конфиденциальной информации;
10. Запрет на использование сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией;
11. Использование лицензированного ПО.

Для уровня программно – аппаратной защиты защиты были выделены следующие термы:

Низкий (1) – устанавливается при использовании печати с маркировкой и системы Screen Guard;

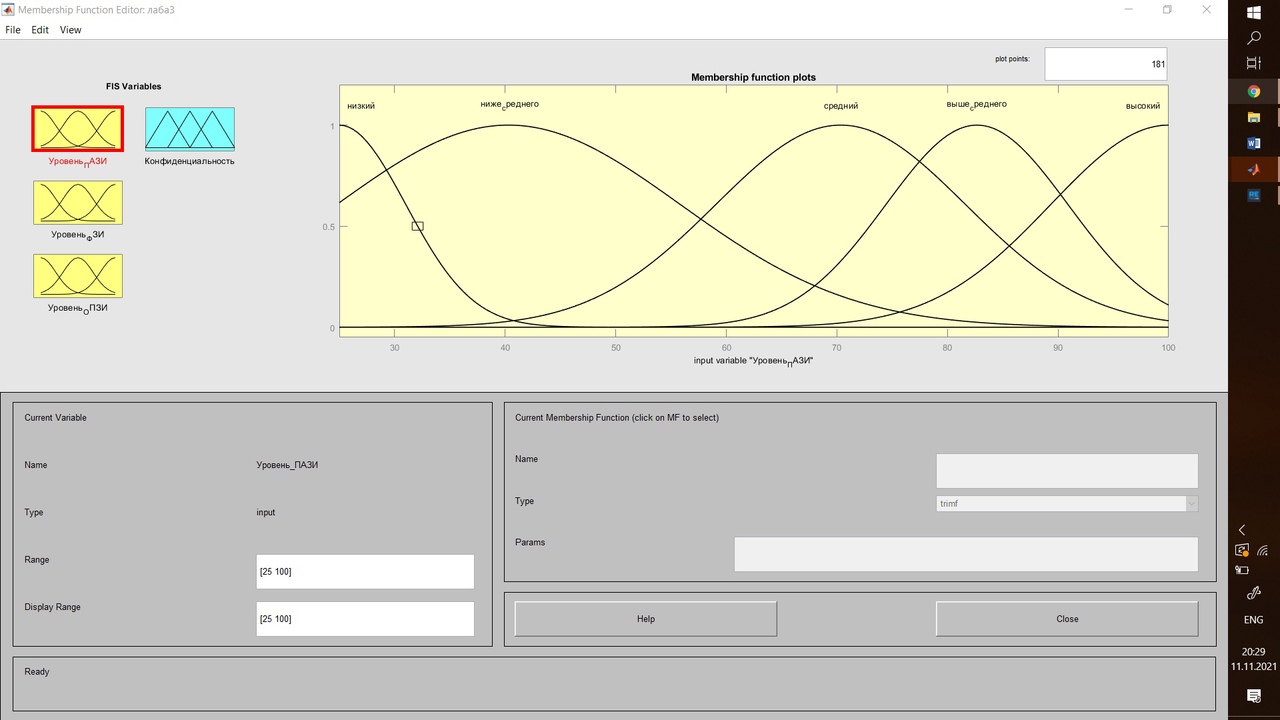
Ниже среднего (2) – устанавливается при использовании методов низкого уровня с использованием аутентификации по SSH для доступа к серверу;

Средний (3) – устанавливается при использовании методом уровня «ниже среднего», а также антивирусного ПО и файрволов и периодического создания бэкапа данных;

Выше среднего (4) – при использовании методов среднего уровня с применением программного средства защиты информации от несанкционированного доступа;

Высокий (5) – устанавливается при использовании методов уровня «выше среднего» с включением аудита файлов с помощью IDS/IPC и отключением портов ПК для предотвращения использования внешних носителей.

На рисунке 3 представлен график данной переменной.

Рисунок 3 – Переменная «Уровень программно – аппаратной защиты»

Для уровня физической защиты были выделены следующие термы:

1. Низкий (1) – устанавливается при использовании одного из методов защиты
2. Средний (2) – устанавливается при использовании двух любых методов защиты
3. Высокий (3) – устанавливается при использовании и внедрении всех предполагаемых методов защиты.

На рисунке 4 представлен график данной лингвистической переменной.

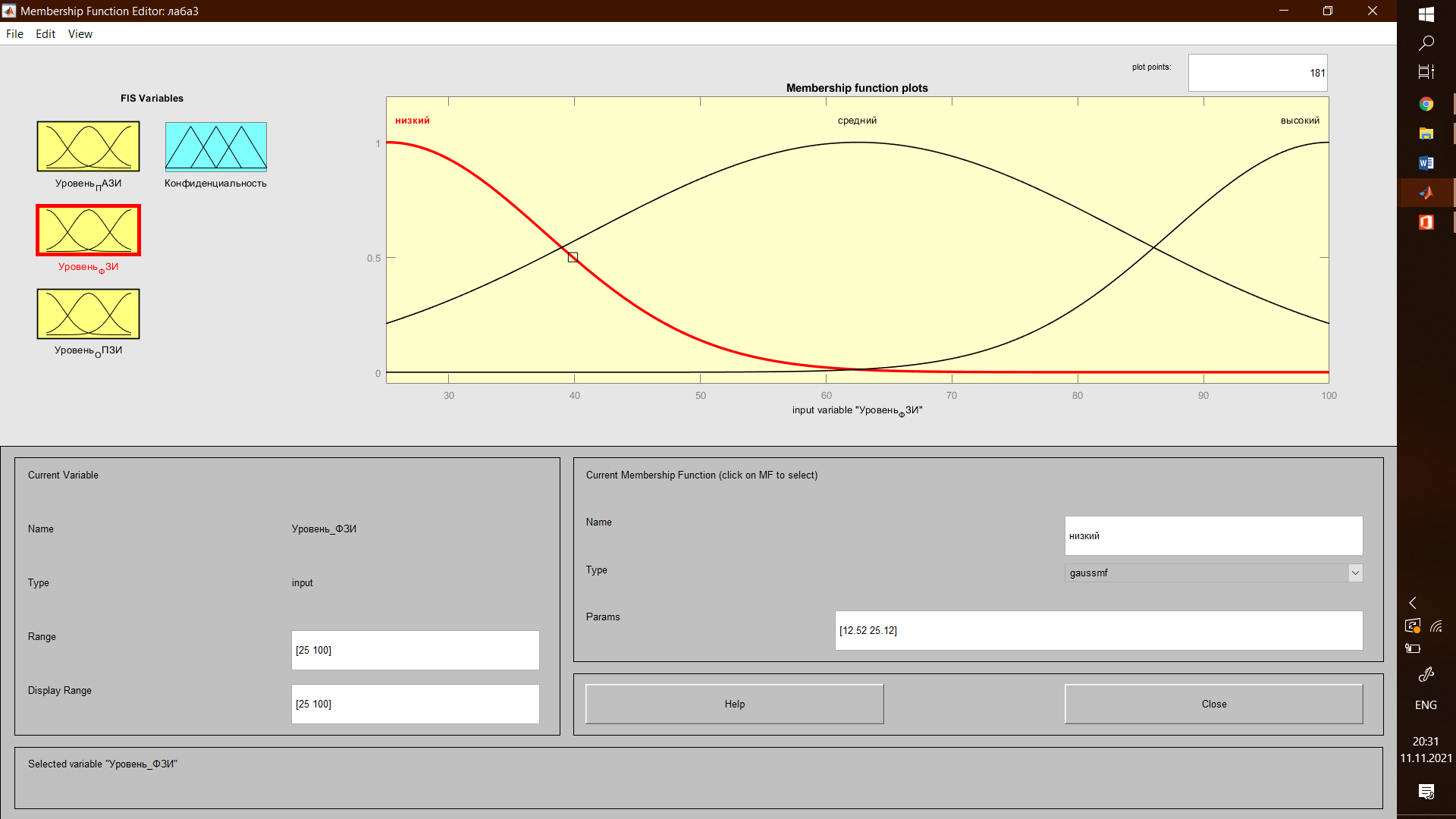


Рисунок 4 – Переменная «Уровень физической защиты»

Для уровня организационно – правовой защиты были выделены следующие термы:

1. Низкий (1) – устанавливается при использовании одного из методов защиты;
2. Средний (2) – устанавливается при использовании двух любых методов защиты;
3. Высокий (3) – устанавливается при использовании и внедрении всех предполагаемых методов защиты.

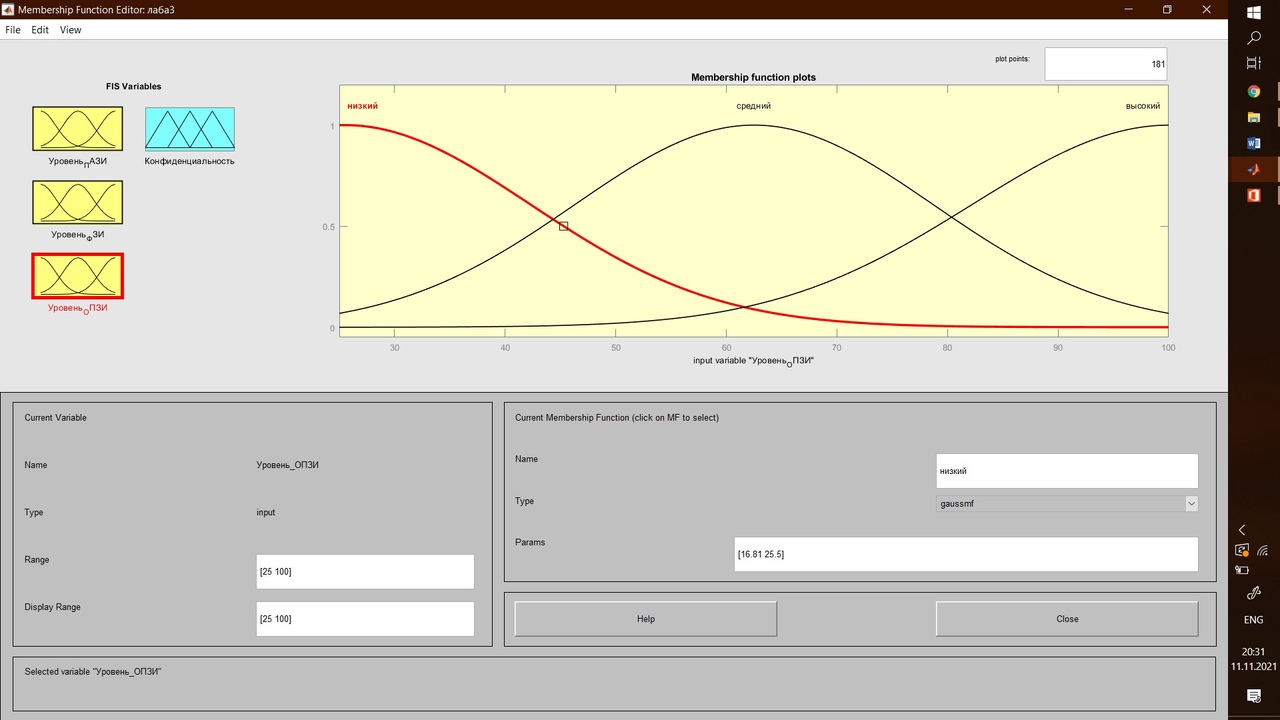
На рисунке 5 представлен график данной переменной.

Рисунок 5 – Уровень организационно – правовой защиты

Основой для проведения операции нечеткого логического вывода является база нечетких правил, содержащая высказывания виды «если …, то …». Входная часть правила находится после слова «если» и называется предпосылкой, выходная, называемая заключением, находится после слова то. В таблице 1 представлена разработанная база правил в наглядном виде.

Таблица 1 – Разработанная база правил.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Уровень ПАЗ | | | | | Уровень физической защиты | | | Уровень организационно – правовой защиты | | | Риск нарушения конфиденциальности |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 1 | 2 | 3 |
| 1 | + | - | - | - | - | + | - | - | + | - | - | Высокий |
| 2 | + | - | - | - | - | + | - | - | - | + | - | Высокий |
| 3 | + | - | - | - | - | + | - | - | - | - | + | Высокий |
| 4 | + | - | - | - | - | - | + | - | + | - | - | Высокий |
| 5 | + | - | - | - | - | - | + | - | - | + | - | Высокий |
| 6 | + | - | - | - | - | - | + | - | - | - | + | Выше среднего |
| 7 | + | - | - | - | - | - | - | + | + | - | - | Высокий |
| 8 | + | - | - | - | - | - | - | + | - | + | - | Выше среднего |
| 9 | + | - | - | - | - | - | - | + | - | - | + | Средний |
| 10 | - | + | - | - | - | + | - | - | + | - | - | Высокий |
| 11 | - | + | - | - | - | + | - | - | - | + | - | Высокий |
| 12 | - | + | - | - | - | + | - | - | - | - | + | Выше среднего |
| 13 | - | + | - | - | - | - | + | - | + | - | - | Высокий |
| 14 | - | + | - | - | - | - | + | - | - | + | - | Высокий |
| 15 | - | + | - | - | - | - | + | - | - | - | + | Выше среднего |
| 16 | - | + | - | - | - | - | - | + | + | - | - | Высокий |
| 17 | - | + | - | - | - | - | - | + | - | + | - | Выше среднего |
| 18 | - | + | - | - | - | - | - | + | - | - | + | Средний |
| 19 | - | - | + | - | - | + | - | - | + | - | - | Высокий |
| 20 | - | - | + | - | - | + | - | - | - | + | - | Высокий |
| 21 | - | - | + | - | - | + | - | - | - | - | + | Высокий |
| 22 | - | - | + | - | - | - | + | - | + | - | - | Выше среднего |
| 23 | - | - | + | - | - | - | + | - | - | + | - | Выше среднего |
| 24 | - | - | + | - | - | - | + | - | - | - | + | Выше среднего |
| 25 | - | - | + | - | - | - | - | + | + | - | - | Выше среднего |
| 26 | - | - | + | - | - | - | - | + | - | + | - | Средний |
| 27 | - | - | + | - | - | - | - | + | - | - | + | Ниже среднего |
| 28 | - | - | - | + | - | + | - | - | + | - | - | Выше среднего |
| 29 | - | - | - | + | - | + | - | - | - | + | - | Выше среднего |
| 30 | - | - | - | + | - | + | - | - | - | - | + | Выше среднего |
| 31 | - | - | - | + | - | - | + | - | + | - | - | Выше среднего |
| 32 | - | - | - | + | - | - | + | - | - | + | - | Средний |
| 33 | - | - | - | + | - | - | + | - | - | - | + | Средний |
| 34 | - | - | - | + | - | - | - | + | + | - | - | Выше среднего |
| 35 | - | - | - | + | - | - | - | + | - | + | - | Средний |
| 36 | - | - | - | + | - | - | - | + | - | - | + | Ниже среднего |
| 37 | - | - | - | - | + | + | - | - | + | - | - | Выше среднего |
| 38 | - | - | - | - | + | + | - | - | - | + | - | Выше среднего |
| 39 | - | - | - | - | + | + | - | - | - | - | + | Выше среднего |
| 40 | - | - | - | - | + | - | + | - | + | - | - | Выше среднего |
| 41 | - | - | - | - | + | - | + | - | - | + | - | Средний |
| 42 | - | - | - | - | + | - | + | - | - | - | + | Ниже среднего |
| 43 | - | - | - | - | + | - | - | + | + | - | - | Выше среднего |
| 44 | - | - | - | - | + | - | - | + | - | + | - | Средний |
| 45 | - | - | - | - | + | - | - | + | - | - | + | Низкий |

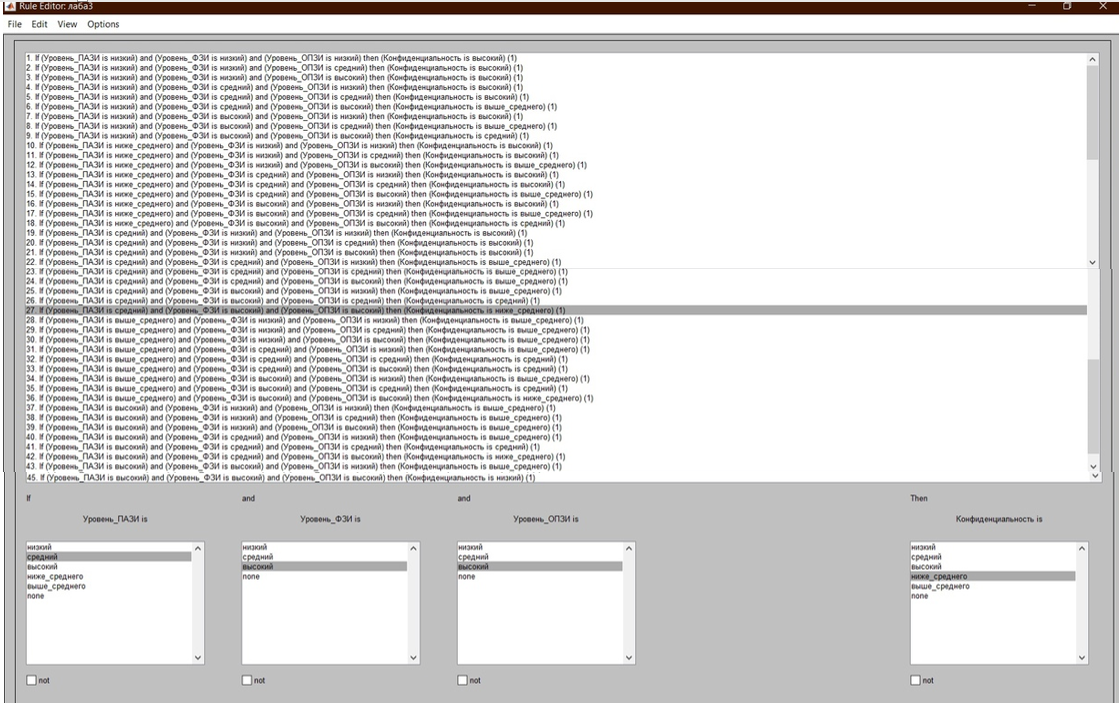
На рисунке 6 продемонстрирована созданная база правил.

Рисунок 6 – Созданная база правил

При анализе полученных данных, можно сделать вывод, что риск нарушения конфиденциальности снижается только в случае комплексной реализации мер защиты.

На рисунках 7 – 8 представлен пример демонстрации корректной работы правил.

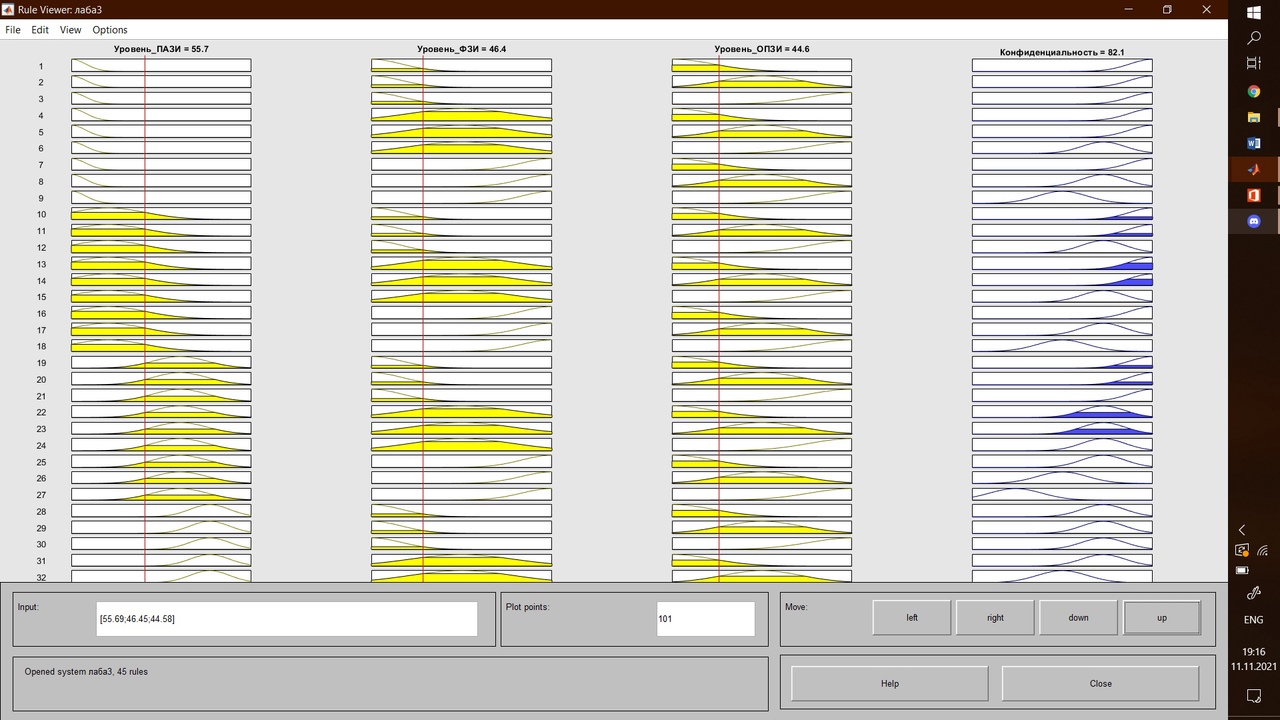
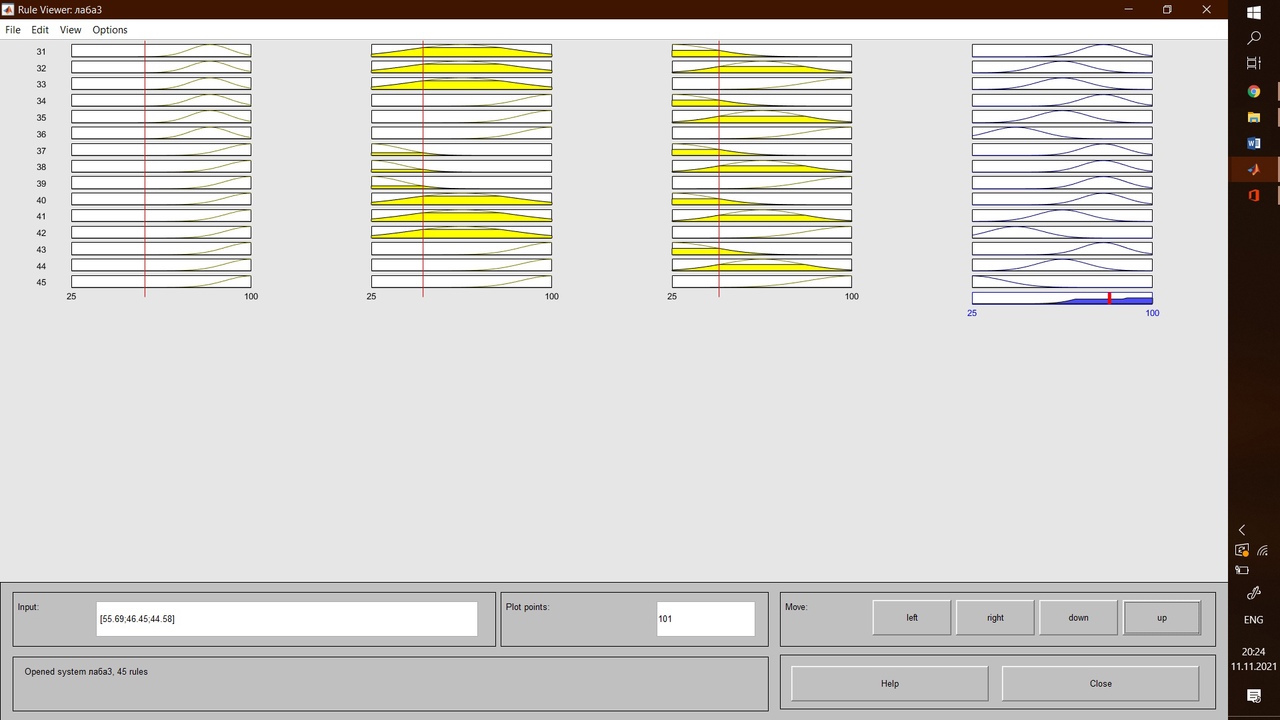
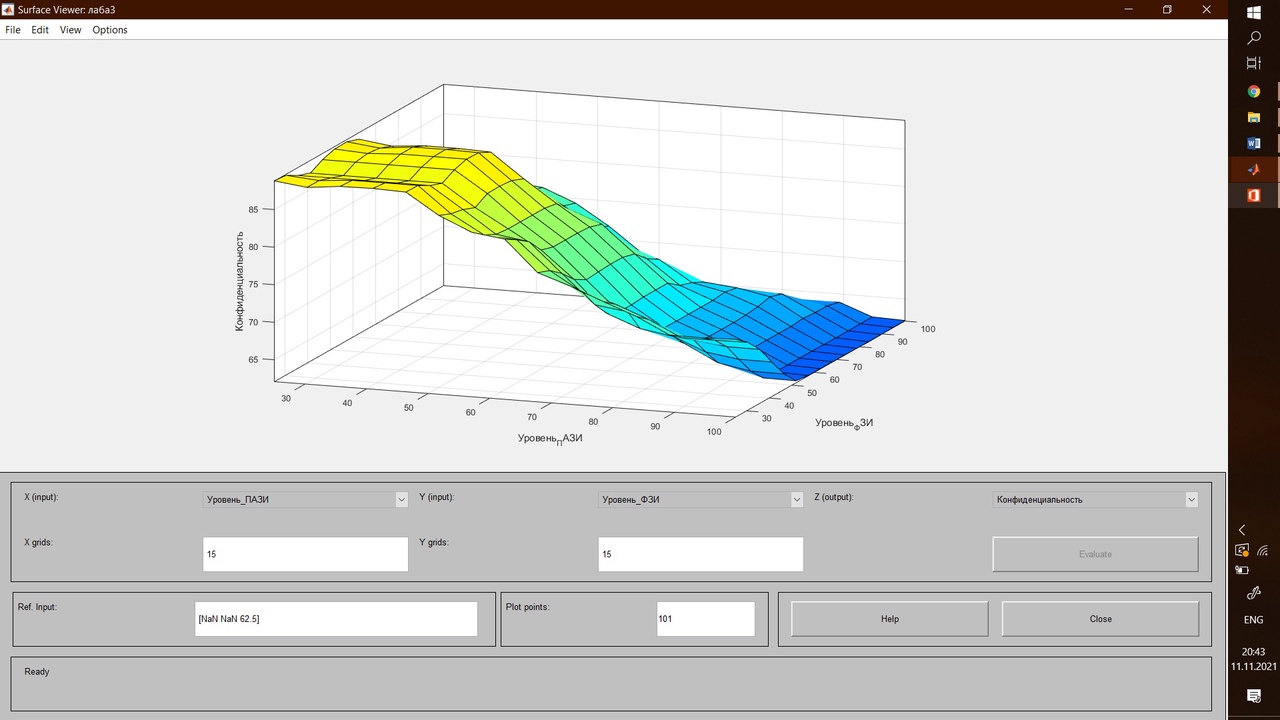
Рисунок 7 – Пример демонстрации корректной работы правил

Рисунок 8 – Пример демонстрации корректной работы правил

 Взаимосвязь переменных различных уровней между собой, то есть реализация методов защиты различных уровней, можно также представить в виде поверхности, построенной по разработанным правилам. Данные поверхности представлены на рисунках 9 – 11.

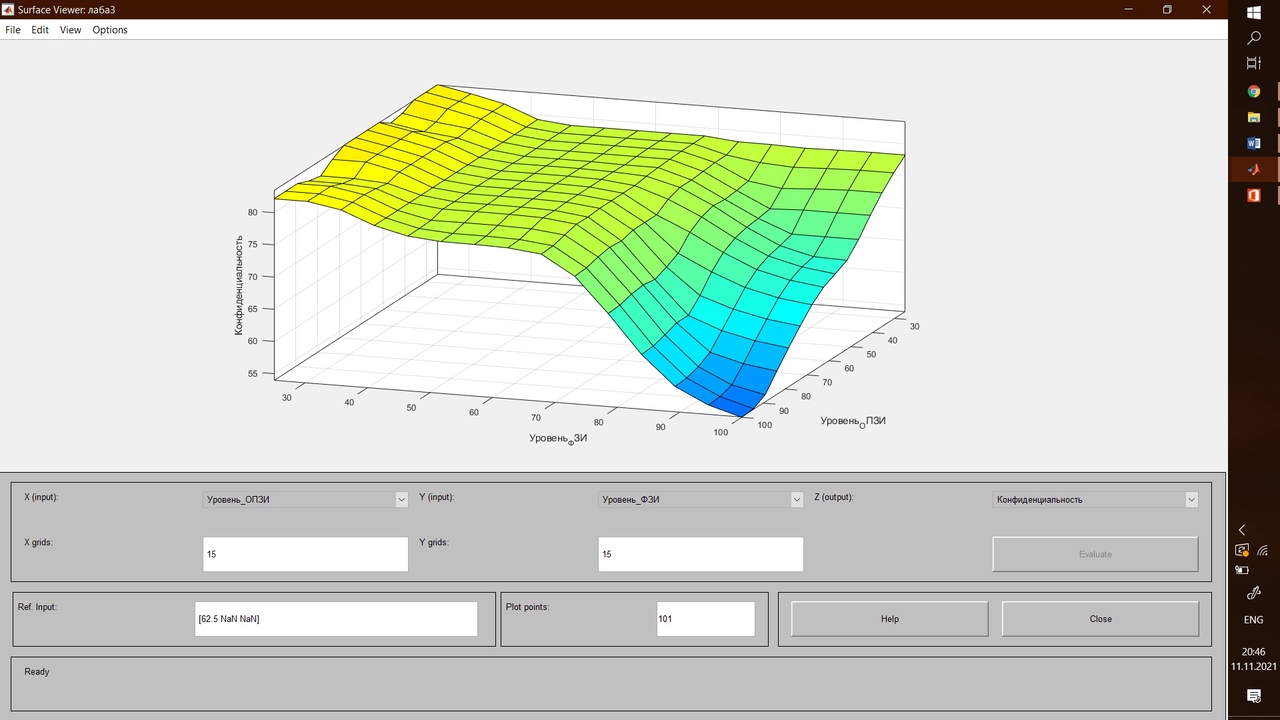
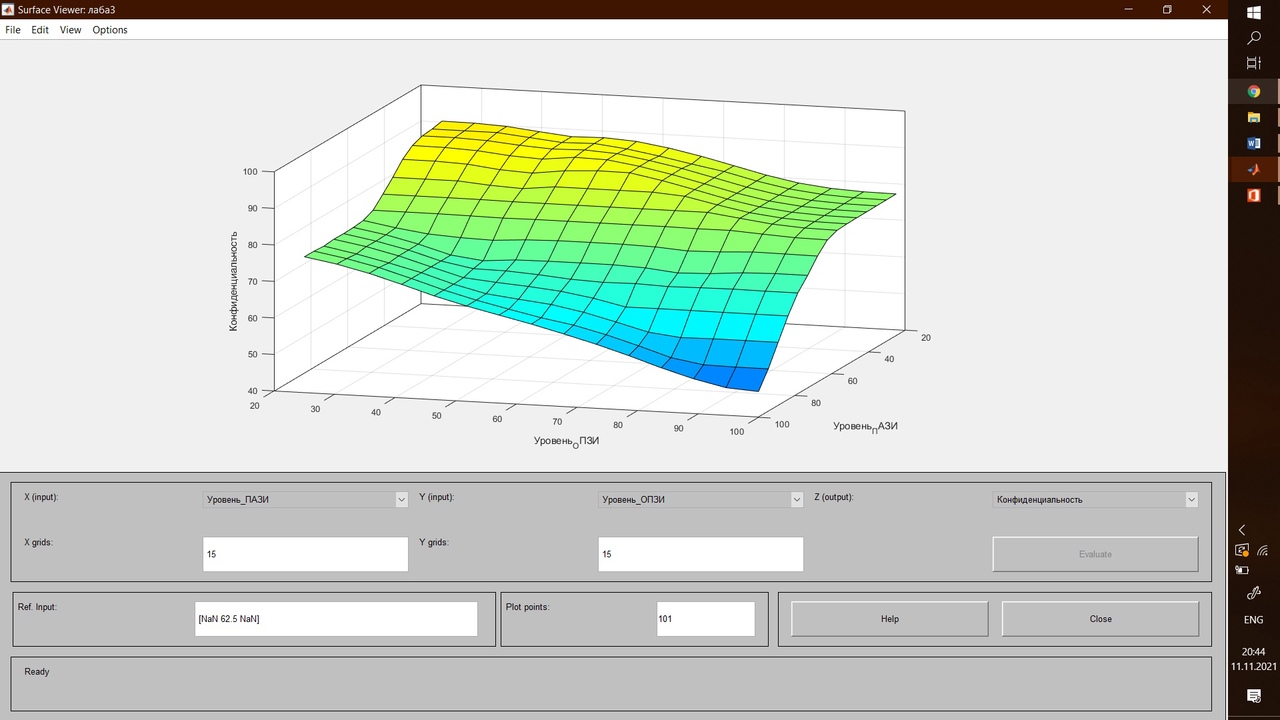
Рисунок 9 – Поверхность, построенная по разработанным правилам

Рисунок 10 – Поверхность, построенная по разработанным правилам

Рисунок 11 – Поверхность, построенная по разработанным правилам

**Выводы:**

В результате выполнения лабораторной работы был проведен системный анализ предметной области. Были оценены различные уровни реализации нескольких мер защиты, таких как, программно – аппаратные, физические и организационно – правовые. Была составлена база нечетких правил, определяющих риск нарушения конфиденциальности данных при различных уровнях реализации методов защиты (Рис. 6)

На основании полученных результатов можно сделать вывод, что риск нарушения конфиденциальности данных снижается только в случае комплексного использования мер защиты.

Список использованных источников

1. Нечеткая логика, URL: <https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%87%D1%91%D1%82%D0%BA%D0%B0%D1%8F_%D0%BB%D0%BE%D0%B3%D0%B8%D0%BA%D0%B0>
2. Нечеткая логика – математические основы, URL: <https://vc.ru/loginom/201212-nechetkaya-logika-matematicheskie-osnovy>
3. Системы нечеткого вывода, URL: <http://nrsu.bstu.ru/chap27.html>
4. Операции нечеткой логики, URL: <https://studme.org/183446/tehnika/operatsii_nechetkoy_logiki>