Министерство образования Республики Беларусь

Учреждение образования

“Брестский государственный технический университет”

Кафедра интеллектуально-информационных технологий

Лабораторная работа №1

“Представление знаний. Продукционная модель”

Выполнил:

студент 3 курса

группы ИИ-23

Романюк А. П.

Проверил:

Савонюк В. А.

Брест 2025

**Вариант 9**

**Задание:**

9. Построить продукционную модель представления знаний в предметной области «Компьютерная безопасность» (угрозы).

**Описание процесса решения.** Для построения продукционной модели представления знаний необходимо выполнить следующие шаги:

1. Определить целевые действия задачи (являющиеся решениями).
2. Определить промежуточные действия или цепочку действий, между начальным состоянием и конечным (являющиеся решениями).
3. Определить условия для каждого действия, при котором его целесообразно и возможно выполнить. Определить порядок выполнения действий.
4. Добавить конкретики при необходимости, исходя из поставленной задачи.
5. Преобразовать полученный порядок действий и соответствующие им условия в продукции.
6. Для проверки правильности построения продукций записать цепочки продукций, явно проследив связи между ними.

Этот набор шагов предполагает движение при построении продукционной модели от результата к начальному состоянию, но возможно и движение от начального состояния к результату.

**Решение**

1. **Определение целевых действий задачи:**  
   Основная цель в предметной области компьютерной безопасности – это предотвращение, обнаружение и устранение угроз. Соответственно, целевыми действиями будут:
   * «предотвратить угрозу»,
   * «обнаружить угрозу»,
   * «устранить последствия угрозы».
2. **Определение цепочки промежуточных действий:**  
   Для достижения этих целей необходимо выполнить ряд промежуточных действий:
   * Определить возможные уязвимости.
   * Выявить потенциальные угрозы (анализировать логи, трафик).
   * Установить средства защиты (межсетевые экраны, антивирусы, системы мониторинга).
   * Оценить уровень риска.
   * Реагировать на обнаруженную угрозу (блокировать, локализовать).
3. **Определение условий и порядка действий:**
   * Прежде чем предотвращать угрозу, нужно определить уязвимость и выявить потенциальные угрозы.
   * Для устранения угрозы необходимо обнаружить ее и локализовать.
   * Все действия выполняются в зависимости от уровня угрозы, типа уязвимости и доступных ресурсов.
4. **Добавление конкретики:**  
   Рассмотрим три типа угроз:
   * Вирусная атака.
   * Атака методом «человек посередине» (Man-in-the-Middle).
   * DDoS-атака.  
     Пусть в системе установлены антивирус, система обнаружения вторжений (IDS) и межсетевой экран.
5. **Преобразование в продукции:**  
   Для представления знаний в форме «Если, то» можно записать:

- Если обнаружена угроза и активность связана с внешней атакой, то активировать защитные меры.

- Если угроза подтверждена и защитные меры активированы, то изолировать сеть.

- Если угроза не подтверждена, но защитные меры активированы, то выполнить анализ системы.

- Если сеть изолирована и выявлены уязвимости, то устранить уязвимости.

- Если выполнен анализ системы и выявлены уязвимости, то оповестить администратора.

- Если администратор оповещен, то начать восстановление системы.

- Если уязвимости устранены, то завершить локализацию угрозы.

- Если начато восстановление системы или завершена локализация угрозы, то выполнить финальную проверку.

- Если выполнена финальная проверка, то завершить процесс обработки инцидента

**Построение модели:**

**Факты (Ф):**  
 **Ф1** – обнаружена угроза.

**Ф2** – угроза подтверждена.

**Ф3** – активность связана с внешней атакой.

**Ф4** – выявлены уязвимости.

**Действия (Д):**  
Д1 – активировать защитные меры.

Д2 – изолировать сеть.

Д3 – выполнить анализ системы.

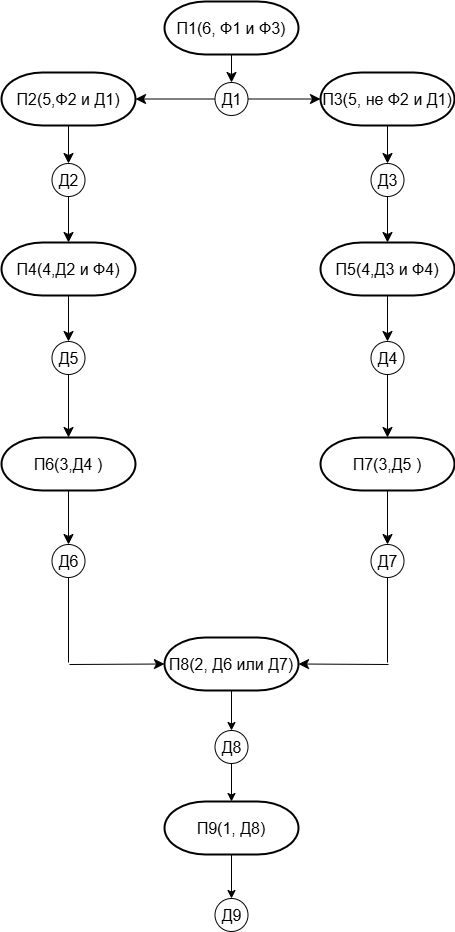
Д4 – оповестить администратора.

Д5 – устранить уязвимости.

Д6 – начать восстановление системы.

Д7 – завершить локализацию угрозы.

Д8 – выполнить финальную проверку.

 Д9 – завершить процесс обработки инцидента.

**Продукции (П):**  
П1(6, Ф1 и Ф3) = Д1.

П2(5, Ф2 и Д1) = Д2.

П3(5, не Ф2 и Д1) = Д3.

П4(4, Д2 и Ф4) = Д5.

П5(4, Д3 и Ф4) = Д4.

П6(3, Д4) = Д6.

П7(3, Д5) = Д7.

П8(2, Д6 или Д7) = Д8.

П9(1, Д8) = Д9.

Для отображения взаимосвязи продукций построим граф.

Вывод: Эта модель позволяет описать процесс работы системы безопасности в виде последовательности действий, которые необходимо выполнить.