Министерство образования Республики Беларусь

Учреждение образования

“Брестский государственный технический университет”

Кафедра интеллектуально-информационных технологий

Лабораторная работа №2

“Представление знаний. Семантическая сеть”

Выполнил:

студент 3 курса

группы ИИ-22

Романюк А. П.

Проверил:

Савонюк В. А.

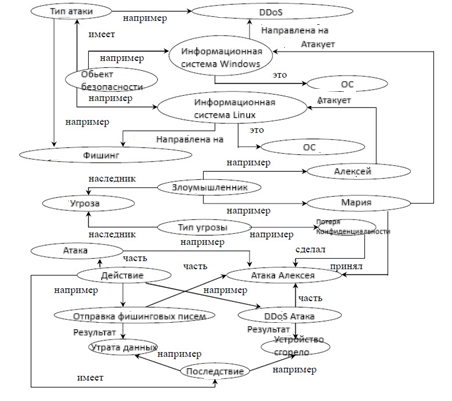
Брест 2025

Задание:

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

**Решение.**

1. Ключевые понятия данной предметной области – это угрозы, системы, которые они могут затронуть (информационные системы), а также субъекты, которые эти угрозы создают (злоумышленники). Системы подвергаются угрозам, которые могут привести к ущербу, поэтому целесообразно выделить общее абстрактное понятие - объект безопасности. Угрозы делятся на различные типы, например, атаки на конфиденциальность, целостность или доступность. Исходя из этого, вершины графа будут следующими: “Объект безопасности”, “Информационная система”, “Угроза”, “Злоумышленник”, “Тип угрозы”, “Последствие”.
2. У этих объектов есть определенные свойства и атрибуты. Например, угрозы имеют определенные типы (атаки на конфиденциальность, целостность, доступность), а также могут быть реализованы конкретными действиями злоумышленников. Поэтому добавим вершины “Тип атаки” и “Действие”.
3. Определим для имеющихся вершин отношения и их типы.
4. Добавим знание о конкретных фактах решаемой задачи. Пусть в данной предметной области есть злоумышленник Алексей, который провел атаку на информационную систему компании “Безопасность”. Угроза связана с утечкой конфиденциальных данных. Тип атаки – фишинг, а последствия – утрата данных и их передача третьим лицам. Последствия реализованы действиями, такими как отправка фишинговых писем.
5. Осуществим проверку установленных связей. Например, возьмем вершину “Угроза” и пройдем по установленным связям. Получаем следующую информацию: угроза относится к информационной системе, является результатом действий злоумышленника, конкретным примером может быть утечка данных, связанная с атакой типа фишинг.



Для получения ответа на какой-либо вопрос по этой задаче необходимо найти соответствующий участок сети и, используя связи, получить результат.

Например, вопрос **«Какие действия реализовал Алексей, чтобы совершить утечку данных?»**  
Из запроса понятно, что необходимо найти следующие вершины: **“Действие”**, **“Алексей”**, и **“Атака”**.

Часть семантической сети, находящаяся между этими вершинами, содержит ответ, а именно:  
утечка данных была связана с отправкой фишинговых писем.

Больше информации в модели нет, поэтому делаем вывод: **действия Алексея включали отправку фишинговых писем**.