Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №7**

По дисциплине «Проектирование баз знаний»

Тема: «Построение онтологии в системе Protégé»

**Выполнил:**

Студент 3 курса

Группы ИИ-21

Карагодин Д.Л.

**Проверил:**

Савонюк В.А.

Брест 2024

**Цель работы:** Получение опыта в анализе предметной области для построения онтологии на основе фреймовой модели в системе Protégé.

**Вариант 2**

**Задание 2.** Онтология по компьютерным вирусам.

**Ход работы:**

**Шаг 1. Определение области и масштаба онтологии**

**Область:** Онтология будет охватывать информацию о компьютерных вирусах, их типах, характеристиках, методах распространения, воздействии на систему.

**Цель использования:** Онтология будет использоваться для классификации и описания компьютерных вирусов, а также для обучения и информирования о них.

**Типы вопросов:** Информация в онтологии должна давать ответы на вопросы о типах вирусов, их характеристиках, методах распространения, вредоносных действиях, методах обнаружения и защиты.

**Пользователи:** Пользователями онтологии могут быть специалисты в области информационной безопасности, разработчики антивирусного программного обеспечения, исследователи в области компьютерных наук и конечные пользователи для получения информации о вирусах и защите от них.

**Масштаб:** Онтология будет содержать основные термины, связанные с компьютерными вирусами, и базовую информацию о них.

**Шаг 2. Рассмотрение вариантов повторного использования существующих онтологий**

Ни один из предложенных вариантов существующих онтологий, не имеет в наличии данную тему онтологии.

**Шаг 3. Перечисление важных терминов в онтологии**

1. **Вирус**
   * **Свойства:** Распространение, Вредоносные действия, Обнаружение, Защита.
   * **Описание:** Программа, способная копировать и распространять себя, нанося вред компьютерной системе.
2. **Троян**
   * **Свойства:** Маскировка, Незаметное внедрение, Вредоносные действия.
   * **Описание:** Вид вируса, скрывающийся под обычной программой, но выполняющий вредные действия при активации.
3. **Вирус-червь**
   * **Свойства:** Автономное распространение, Сетевые уязвимости, Масштабные атаки.
   * **Описание:** Вирус, который способен самостоятельно распространяться по сети и заражать другие устройства.
4. **Руткит**
   * **Свойства:** Скрытность, Привилегированный доступ, Обход защиты.
   * **Описание:** Программа, скрывающая присутствие других вредоносных программ и предоставляющая им привилегированный доступ к системе.
5. **Адвар (Adware)**
   * **Свойства:** Реклама, Сбор информации о пользователе.
   * **Описание:** Программа, отображающая рекламные объявления без согласия пользователя и часто собирающая информацию о его действиях в сети.
6. **Спайвар (Spyware)**
   * **Свойства:** Шпионаж, Перехват данных, Незаконный доступ.
   * **Описание:** Программа, собирающая информацию о пользователе без его согласия и передающая её третьим лицам.
7. **Рансомвар (Ransomware)**
   * **Свойства:** Шифрование данных, Вымогательство, Отправка требований выкупа.
   * **Описание:** Вирус, шифрующий данные на зараженном устройстве и требующий выкуп для их разблокировки.
8. **Ботнет**
   * **Свойства:** Удаленное управление, Масштабные атаки, Компьютерная сеть.
   * **Описание:** Сеть компьютеров, зараженных вирусами, которые могут быть удаленно управляемыми злоумышленниками.
9. **Кейлоггер**
   * **Свойства:** Запись нажатий клавиш, Перехват данных.
   * **Описание:** Программа, записывающая все нажатия клавиш на зараженном устройстве и передающая полученные данные злоумышленникам.

**Неформальная группировка:** Вирус имеет в себе Троян, Вирус-Червь, Руткит, Сетевой вирус; Малваре имеет в себе Адвар, Спайвар, Рансомвар; Кейлоггер и Ботнет сами по себе.

**Шаг 4. Определение классов и иерархии классов**

Компьютерный вирус:

1. Вирус:

1.1. Троян;

1.2. Вирус-червь;

1.3. Руткит;

1.4. Сетевой вирус.

1. Малваре (Вредоносное ПО):

2.1. Адвар (Adware);

2.2. Спайвар (Spyware);

2.3. Рансомвар (Ransomware).

1. Кейлоггер:
2. Ботнет.

**Шаг 5,6. Определение свойств классов – слотов. Определение фацетов слотов (ограничений на слоты)**

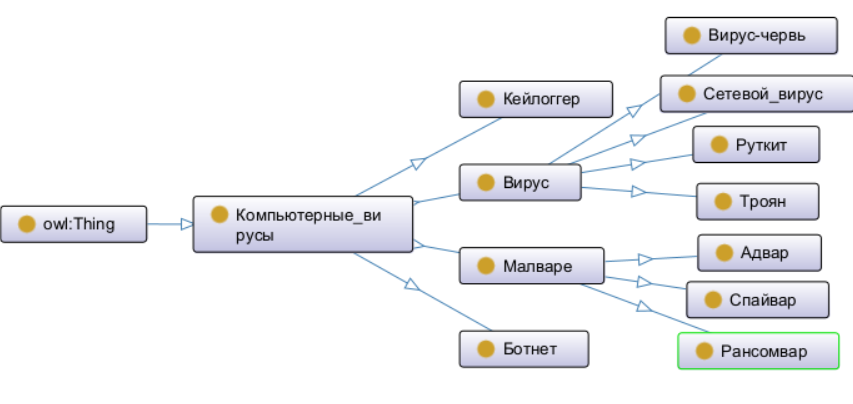
**Компьютерный вирус**

* + **имя** (строка) - Имя вируса
  + **размер** (целое число) - Размер вируса в байтах
  + **опасность** (целое число) - Уровень опасности (минимум: 1, максимум: 10, значение по умолчанию: 5)
  + **распространение** (булево значение) - Может ли распространяться самостоятельно
  + **Подклассы:**

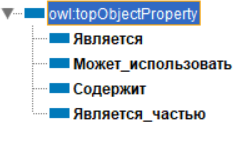
1. **Вирус**
   * **метод инфекции** (строка) - Описывает способ, с помощью которого вирус инфицирует систему (например, внедрение в исполняемые файлы, маскировка под системные процессы).
   * **Подклассы:**
     + **Троян**:
       - **задача** (строка) - Задача, выполняемая трояном (например, шпионаж, уничтожение данных)
       - **скрытность\_активности** (булево значение) - Возможность трояна скрывать свою активность
     + **Вирус-червь**:
       - **метод\_распространения** (строка) - Метод распространения вируса (например, через уязвимости сетевых протоколов)
       - **количество\_зараженных\_компьютеров** (целое число) - Количество компьютеров, зараженных вирусом-червем
     + **Руткит**:
       - **маскировка** (строка) - Методы маскировки в системе (например, изменение системных вызовов, скрытие файлов и процессов)
       - **привилегии** (строка) - Уровень привилегий, к которому руткит может получить доступ
     + **Сетевой вирус**:
       - **цель\_атаки** (строка) - Цель атаки для сетевого вируса (например, сетевые узлы, серверы)
       - **скорость\_распространения** (строка) - Скорость распространения в сети (например, быстро, медленно)
2. **Малваре (Вредоносное ПО)**
   * + **Метод распространения** (строка) -Указывает на метод, используемый для распространения вредоносного ПО (например, через вредоносные веб-сайты, через всплывающие окна).
   * **Подклассы:**
     + **Адвар (Adware)**:
       - **рекламные\_баннеры** (список строк) - Список рекламных баннеров, отображаемых адваром
       - **тип\_рекламы** (строка) - Тип рекламы, отображаемой адваром (например, всплывающие окна, баннеры)
     + **Спайвар (Spyware)**:
       - **цель\_подслушивания** (строка) - Цель подслушивания для спайвара (например, личные данные, пароли)
       - **метод\_передачи\_информации** (строка) - Метод передачи украденной информации (например, почта, удаленный сервер)
     + **Рансомвар (Ransomware)**:
       - **вымогаемая\_сумма** (целое число) - Сумма, требуемая в качестве выкупа за разблокировку данных
       - **способ\_оплаты** (строка) - Способ оплаты выкупа (например, криптовалюта, банковский перевод)
3. **Кейлоггер**
   * + - **захваченные\_данные** (строка) - Тип захватываемых данных (например, нажатия клавиш, данные форм)
       - **метод\_записи** (строка) - Метод записи захваченных данных (например, локальное хранение, отправка на удаленный сервер)
4. **Ботнет**
   * + **Распределенная инфраструктура** (булево значение): Указывает, использует ли ботнет распределенную инфраструктуру для управления зараженными устройствами.

**Результат работы в программе:**

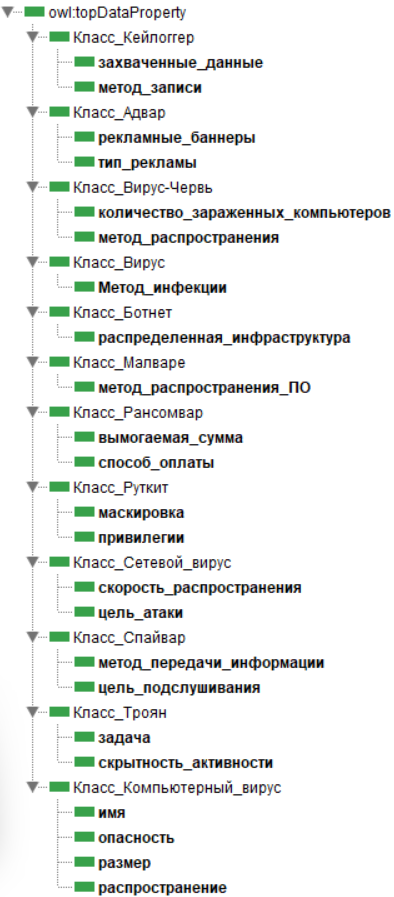
**Создание классов и её иерархии:**

****

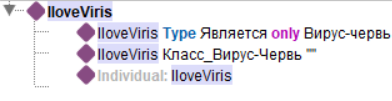
**Создание отношений в классе:**

****

**Создание свойств для классов:**

****

**Пример создания вируса:**

****

**Вывод:** Получил опыт в анализе предметной области для построения онтологии на основе фреймовой модели в системе Protégé.