Министерство науки и высшего образования РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

институт

Кафедра прикладной информатики

кафедра

**ОТЧЕТ О ПРАКТИЧЕСКОЙ РАБОТЕ № 4**

Интеллектуальный анализ данных

наименование дисциплины

Фреймовая модель (вариант 9)

тема (вариант)

Преподаватель \_\_\_\_\_\_\_\_\_\_ Т.Н. Сизова

подпись, дата инициалы, фамилия

Студент КИ22-21б 032215739 \_\_\_\_\_\_\_\_\_\_ А.С. Полешко

номер группы номер зачетной книжки подпись, дата инициалы, фамилия

Красноярск 2025

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc192003516)

[Ход работы 4](#_Toc192003517)

[ЗАКЛЮЧЕНИЕ 9](#_Toc192003518)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 12](#_Toc192003519)

# **ВВЕДЕНИЕ**

Цель работы: получение знаний, умений и навыков по созданию базы знаний, представляющей собой фреймовую модель.

# **Ход работы**

Описание задачи: построить фреймовую модель представления знаний в предметной области «Компьютерная безопасность» (угрозы).

Для построения фреймовой модели представления знаний необходимо выполнить следующие шаги:

1) определить абстрактные объекты и понятия предметной области, необходимые для решения поставленной задачи. Оформить их в виде фреймов-прототипов (фреймов-объектов, фреймов-ролей);

2) задать конкретные объекты предметной области. Оформить их в виде фреймов-экземпляров (фреймов-объектов, фреймов-ролей);

3) определить набор возможных ситуаций. Оформить их в виде фреймов-ситуаций (прототипы). Если существуют прецеденты по ситуациям в предметной области, добавить фреймы-экземпляры (фреймы-ситуации);

4) описать динамику развития ситуаций (переход от одних к другим) через набор сцен. Оформить их в виде фреймов-сценариев;

5) добавить фреймы-объекты сценариев и сцен, которые отражают данные конкретной задачи.

Решение.

1) Предметная область включает такие понятия, как оружие, злоумышленник, метод защиты, информационная система (ИС) и последствие. Тогда можно выделить фреймы-прототипы: «Оружие», «Злоумышленник», «Метод защиты», «Информационная система», «Последствие». Также нужно определить основные слоты фреймов – характеристики, имеющие значения для решаемой задачи.

|  |  |  |  |
| --- | --- | --- | --- |
| **ОРУЖИЕ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Тип |  | из внешних источников |  |
| Уязвимость |  | из внешних источников |  |
| Эффективность | Низкая, средняя или высокая | из внешних источников |  |
| Механизм распространения |  | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ЗЛОУМЫШЛЕННИК** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Мотив |  | из внешних источников |  |
| Оружие | Фрейм-объект | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **МЕТОД ЗАЩИТЫ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Тип |  | из внешних источников |  |
| Эффективность | Низкая, средняя или высокая | из внешних источников |  |
| Порог внедрения | Низкий, средний или высокий | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ИНФОРМАЦИОННАЯ СИСТЕМА** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Сфера |  | из внешних источников |  |
| Уязвимости |  | из внешних источников |  |
| Методы защиты | Фрейм-объекты | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ПОСЛЕДСТВИЕ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Затронутая система | Фрейм-объект | из внешних источников |  |
| Экономический ущерб, руб. |  | из внешних источников |  |

2) Фреймы-образцы описывают конкретную ситуацию: кто является злоумышленником, и какое оружие они используют. На какие ИС осуществляется атака, а также какие методы защиты используются. Поэтому определим следующие фреймы-образцы, являющиеся наследниками фреймов-прототипов:

2.1) Образцы оружия

|  |  |  |  |
| --- | --- | --- | --- |
| **ВИРУС-ВЫМОГАТЕЛЬ «WANNACRY» (**AKO **ОРУЖИЕ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Тип | Вымогательское ПО (Ransomware) | из внешних источников |  |
| Уязвимость | Устаревшее ПО | из внешних источников |  |
| Эффективность | Высокая | из внешних источников |  |
| Механизм распространения | Самораспространение | из внешних источников |  |

2.2) Образцы злоумышленников

|  |  |  |  |
| --- | --- | --- | --- |
| **ХАКЕРСКАЯ ГРУППА «SHADOW BROKERS» (**AKO **ЗЛОУМЫШЛЕННИК)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Мотив | Финансовая выгода | из внешних источников |  |
| Оружие | **ВИРУС-ВЫМОГАТЕЛЬ «WANNACRY»** | из внешних источников |  |

2.3) Образцы методов защиты

|  |  |  |  |
| --- | --- | --- | --- |
| **ОБНОВЛЕНИЕ ПО (**AKO **МЕТОД ЗАЩИТЫ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Тип | Превентивный | из внешних источников |  |
| Эффективность | Средняя | из внешних источников |  |
| Порог внедрения | Средний | из внешних источников |  |

2.4) Образцы ИС

|  |  |  |  |
| --- | --- | --- | --- |
| **ИНФОРМАЦИОННАЯ СИСТЕМА БОЛЬНИЦЫ (**АКО **ИНФОРМАЦИОННАЯ СИСТЕМА)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Сфера | Медицина | из внешних источников |  |
| Уязвимости | Устаревшее ПО | из внешних источников |  |
| Методы защиты | **ОБНОВЛЕНИЕ ПО** | из внешних источников |  |

2.5) Образцы последствий

|  |  |  |  |
| --- | --- | --- | --- |
| **ПОТЕРЯ ДОСТУПА К МЕДИЦИНСКИМ ДАННЫМ (**АКО **ПОСЛЕДСТВИЕ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Затронутая система | **ИНФОРМАЦИОННАЯ СИСТЕМА БОЛЬНИЦЫ** | из внешних источников |  |
| Экономический ущерб, руб. | 4,000,000 | из внешних источников |  |

3) Фреймы-ситуации описывают возможные ситуации (содержат набор характеристик, идентифицирующих ситуацию). Опишем несколько типичных ситуаций: атака на систему и устранение атаки.

|  |  |  |  |
| --- | --- | --- | --- |
| **АТАКА** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Инициатор | Фрейм-образец | из внешних источников |  |
| Оружие | Фрейм-образец | из внешних источников |  |
| Цель | Фрейм-образец | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **УСТРАНЕНИЕ АТАКИ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Метод защиты | Фрейм-образец | из внешних источников |  |
| Последствия | Фрейм-образец | из внешних источников |  |

4) Ситуации возникают после наступления каких-то событий, выполнения условий и могут следовать одна за другой. Динамику предметной области можно отобразить в фреймах-сценариях. Опишем сценарий инцидента.

|  |  |  |  |
| --- | --- | --- | --- |
| **ИНЦИДЕНТ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Сцена 1 | Подготовка атаки | из внешних источников |  |
| Атака | Фрейм-образец | из внешних источников |  |
| Сцена 2 | Обнаружение атаки | из внешних источников |  |
| Устранение атаки | Фрейм-образец | из внешних источников |  |
| Сцена 3 | Оценка последствий | из внешних источников |  |
| Сцена 4 | Улучшение системы | из внешних источников |  |

5) Пусть в рамках нашей задачи хакерская группа «shadow brokers» начинает распространение вредоносного ПО на информационную систему больницы с помощью вируса-вымогателя «WannaCry». В свою очередь ИС должна обнаружить и устранить атаку. Тогда фреймы будут заполнены следующим образом:

|  |  |  |  |
| --- | --- | --- | --- |
| **ИНЦИДЕНТ «WANNACRY» В РФ** **(**АКО **ИНЦИДЕНТ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Сцена 1 | Подготовка атаки | из внешних источников |  |
| Атака | **РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПО** | из внешних источников |  |
| Сцена 2 | Обнаружение атаки | из внешних источников |  |
| Устранение атаки | **УСТРАНЕНИЕ АТАКИ «WANNACRY»** | из внешних источников |  |
| Сцена 3 | Оценка последствий | из внешних источников |  |
| Сцена 4 | Улучшение системы | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПО (**АКО **АТАКА)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Инициатор | **ХАКЕРСКАЯ ГРУППА «SHADOW BROKERS»** | из внешних источников |  |
| Оружие | **ВИРУС-ВЫМОГАТЕЛЬ «WANNACRY»** | из внешних источников |  |
| Цель | **ИНФОРМАЦИОННАЯ СИСТЕМА БОЛЬНИЦЫ** | из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **УСТРАНЕНИЕ АТАКИ «WANNACRY» (**АКО **УСТРАНЕНИЕ АТАКИ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Метод защиты | **ОБНОВЛЕНИЕ ПО** | из внешних источников |  |
| Последствия | **ПОТЕРЯ ДОСТУПА К МЕДИЦИНСКИМ ДАННЫМ** | из внешних источников |  |

Взаимосвязь различных видов фреймов отображается графически в виде графа (рисунок 1).

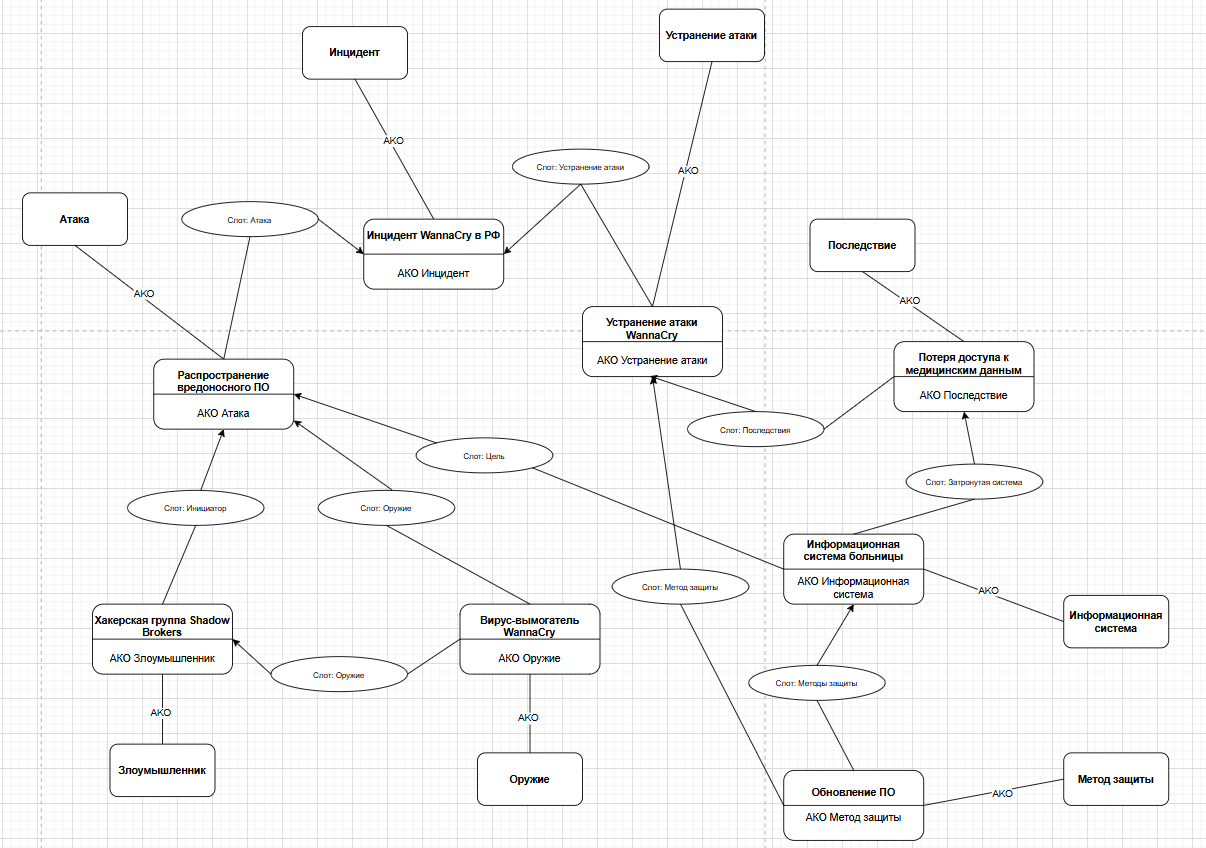


Рисунок 1 – Схема фреймов для предметной области «Компьютерная безопасность»

# **ЗАКЛЮЧЕНИЕ**

В ходе выполнения работы были получены знания, умения и навыки по созданию базы знаний, представляющей собой фреймовую модель.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Электронный курс образовательной программы по дисциплине «Интеллектуальный анализ данных» // Система электронного обучения Сибирского Федерального университета: [сайт]. – Красноярск, 2010 – . – URL: <https://e.sfu-kras.ru/course/view.php?id=1109> (дата обращения: 8.04.2025). – Режим доступа: для авториз. пользователей. – Текст: электронный.