Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №3**

По дисциплине «Проектирование баз знаний»

Тема: «Представление знаний. Фреймовая модель»

**Выполнил:**

Студент 3 курса

Группы ИИ-23

Романюк А. П.

**Проверил:**

Савонюк В.А.

Брест 2025

**Цель работы:** Изучение и решение заданий по составлению фреймовой модели и представлении знаний.

**Ход работы:**

**Вариант 9**

Построить продукционную модель представления знаний в предметной области «Туристическое агентство» (работа с клиентами).

**Описание процесса решения.**

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.

**Ход работы:**

1. Ключевые понятия данной предметной области – системы безопасности, потенциальные угрозы (вредоносные субъекты, например, хакеры) и те кто от них защищает (киберспециалист). У хакеров и киберспециалистов есть общие характеристики, поэтому целесообразно выделить общее абстрактное понятие – человек. Тогда фреймы «Система безопасности» и «Человек» являются прототипами-образцами, а фреймы «Хакер» и «Киберспециалист» - прототипами-ролями. Также нужно определить основные слоты фреймов – характеристики, имеющие значения для решаемой задачи.

|  |  |  |  |
| --- | --- | --- | --- |
| **ЧЕЛОВЕК** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Пол | Мужской или Женский | Из внешних источников |  |
| Возраст | От 0 до 110 лет | Из внешних источников |  |
|  | | | |
| **СИСТЕМА БЕЗОПАСНОСТИ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Название |  | Из внешних источников |  |
| IP Адрес |  | Из внешних источников |  |
| Способ работы |  | Из внешних источников |  |
| Направление |  | Из внешних источников |  |
| **КИБЕРСПЕЦИАЛИСТ (**AKO **ЧЕЛОВЕК)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Возраст | От 18 до 55 лет | Из внешних источников |  |
| Стаж работы | От 0 до 60 лет | Из внешних источников |  |
| Зарплата |  | Из внешних источников |  |
| График работы |  | Из внешних источников |  |
| Место работы | Фрейм-Объект | Из внешних источников |  |
|  | | | |
| **ХАКЕР (**AKO **ЧЕЛОВЕК)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Вид атаки | Фишинг или DDoS | По умолчанию (DDoS) |  |
| Форма эксплуатации | Есть или нет | По умолчанию (нет) |  |

1. Фреймы-образцы описывают конкретную ситуацию: какие системы безопасности имеются в организации, кем именно организовывается защита, кто является хакером, кто т.д. Поэтому определим следующие фреймы-образцы, являющиеся наследниками фреймов-прототипов:

|  |  |  |  |
| --- | --- | --- | --- |
| **Система безопасности "SecureNet" (**AKO **СИСТЕМА БЕЗОПАСНОСТИ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Название | SecureNet | Из внешних источников |  |
| IP Адрес | 192.168.3.56 | Из внешних источников |  |
| Способ работы | Многоуровневая аутентификация | Из внешних источников |  |
| Направление | Корпоративная безопасность | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Система безопасности "GuardShield" (**AKO **СИСТЕМА БЕЗОПАСНОСТИ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Название | GuardShield | Из внешних источников |  |
| IP Адрес | 178.3.5.123 | Из внешних источников |  |
| Способ работы | ИИ мониторинг | Из внешних источников |  |
| Направление | Защита сетевой инфраструктуры | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **СЕРГЕЙ (**AKO **КИБЕРСПЕЦИАЛИСТ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Пол | Мужской | Из внешних источников |  |
| Возраст | 31 | Из внешних источников |  |
| Стаж работы | 5 | Из внешних источников |  |
| Зарплата | 1300 | Из внешних источников |  |
| График работы | 6:30 – 13:30 | Из внешних источников |  |
| Место работы | **Система безопасности "SecureNet"** | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **МАРИНА (**AKO **КИБЕРСПЕЦИАЛИСТ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Пол | Женский | Из внешних источников |  |
| Возраст | 31 | Из внешних источников |  |
| Стаж работы | 8 | Из внешних источников |  |
| Зарплата | 1800 | Из внешних источников |  |
| График работы | 14:00 – 00:00 | Из внешних источников |  |
| Место работы | **Система безопасности "GuardShield"** | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **АНДРЕЙ (**AKO **ХАКЕР)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Вид атаки | DDoS | По умолчанию (наличные) |  |
| Форма эксплуатации | есть | По умолчанию (заказа нет) |  |
| Пол | Мужской | Из внешних источников |  |
| Возраст | 20 | Из внешних источников |  |

1. Фреймы-ситуации описывают возможные ситуации. В системе безопасности пользователь может столкнуться с несколькими типичными ситуациями: атака и эксплуатация. Возможны и другие нетипичные ситуации: утечка данных, взлом системы и т.д. Рассмотрим типичные ситуации:

|  |  |  |  |
| --- | --- | --- | --- |
| **АТАКА** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Список уязвимых узлов |  | Из внешних источников | IF-ADDED (изменяет слот «Список доступных эксплойтов») |
| Список доступных эксплойтов |  | Присоединенная процедура | IF-ADDED (изменяет слот «Общий объём данных») |
| Общий объём данных |  | Присоединенная |  |
| Отбивал атаку | Фрейм-образец | Из внешних источников |  |
| Запустил атаку | Фрейм-образец | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ЭКСПЛУАТАЦИЯ** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Метод доступа |  | Из внешних источников |  |
| Исполнил атаку | Фрейм-образец | Присоединенная процедура |  |
| Атака | Фрейм-образец | Из внешних источников |  |

1. Ситуации возникают после наступления каких-то событий, выполнения условий и могут следовать одна за другой. Динамику предметной области можно отобразить в фреймах-сценариях. Их может быть множество, опишем наиболее общий и типичный сценарий обеспечения безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| АТАКА СИСТЕМЫ БЕЗОПАСНОСТИ | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Хакер | Фрейм-объект | Из внешних источников |  |
| Система безопасности | Фрейм-объект | Из внешних источников | IF-ADDED,IF-REMOVED (изменяет слот « Киберспециалист ») |
| Киберспециалист | Фрейм-объект | Присоединённая процедура (определяется по выбранной системе безопасности) |  |
| Сцена 1 | Обнаружение уязвимости | Из внешних источников |  |
| Сцена 2 | Атака | Из внешних источников |  |
| Сцена 3 | Анализ и выбор эксплойтов | Из внешних источников |  |
| Сцена 4 | Эксплуатация | Из внешних источников |  |
| Сцена 5 | Эксфильтрация данных | Из внешних источников |  |

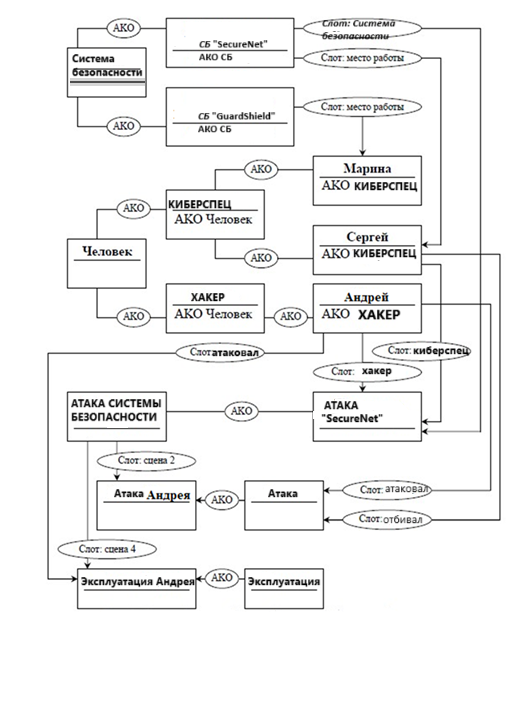
1. Пусть в рамках нашей задачи Андрей атакует систему безопасности. Тогда фреймы будут заполнены следующим образом:

|  |  |  |  |
| --- | --- | --- | --- |
| **АТАКА «SecureNet»** (АКО **АТАКА СИСТЕМЫ БЕЗОПАСНОСТИ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Хакер | АНДРЕЙ | Из внешних источников |  |
| Система безопасности | " **SecureNet** " | Из внешних источников | IF-ADDED,IF-REMOVED (изменяет слот «Киберспециалист») |
| Киберспециалист | СЕРГЕЙ | Присоединённая процедура (определяется по выбранной системе безопасности) |  |
| Сцена 1 | Обнаружение уязвимости | Из внешних источников |  |
| Сцена 2 | Атака | Из внешних источников |  |
| Сцена 3 | Анализ и выбор эксплойтов | Из внешних источников |  |
| Сцена 4 | Эксплуатация | Из внешних источников |  |
| Сцена 5 | Эксфильтрация данных | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **АТАКА АНДРЕЯ** (АКО АТАКА**)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Список уязвимых узлов | Серверы базы данны | Из внешних источников | IF-ADDED (изменяет слот «Список доступных эксплойтов») |
| Список доступных эксплойтов | 3500 | Присоединенная процедура | IF-ADDED (изменяет слот «Общий объём данных») |
| Общий объём данных | 70 | Присоединенная |  |
| Отбивал атаку | СЕРГЕЙ | Из внешних источников |  |
| Запустил атаку | АНДРЕЙ | Из внешних источников |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ЭКСПЛУАТАЦИЯ АНДРЕЯ** (АКО **ЭКСПЛУАТАЦИЯ)** | | | |
| **Имя слота** | **Значение слота** | **Способ получения значения** | **Демон** |
| Метод доступа | Картой | Из внешних источников |  |
| Исполнил атаку | АНДРЕЙ | Присоединенная процедура |  |
| Атака | АТАКА АНДРЕЯ | Из внешних источников |  |

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



*Рис. 1. Схема фреймов для предметной области «Турагенства».*

**Вывод:** изучил и решил задание по составлению фреймовой модели и представлении знаний.