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 № 2**

Интеллектуальный анализ данных

наименование дисциплины

Продукционная 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](#_Toc191398185)

[Ход работы 4](#_Toc191398186)

[Часть 1. 4](#_Toc191398187)

[Часть 2. 8](#_Toc191398188)

[ЗАКЛЮЧЕНИЕ 12](#_Toc191398189)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 13](#_Toc191398190)

# **ВВЕДЕНИЕ**

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

# **Ход работы**

## Часть 1.

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

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 (между тем, что имеется, и целевым действием);

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 (шаги 1 и 2).

**Решение.**

1) Целевое действие в данной области – обеспечение защиты системы от угроз.

2) Прежде чем достичь целевого действия, необходимо выполнить ряд промежуточных шагов, которые помогут выявить, оценить и устранить угрозы:

* идентификация типа угрозы – классификация обнаруженной аномальной активности (вредоносное ПО, атаки, фишинг и т. д.);
* оценка уровня критичности угрозы – определение, насколько серьёзны возможные последствия;
* принятие мер по нейтрализации угрозы – блокировка вредоносной активности, обновление ПО, изменение конфигурации безопасности.

3) Для корректного функционирования системы защиты необходимо определить условия, при которых каждое действие выполняется:

* если в системе зафиксирована аномальная активность (резкое увеличение трафика, неизвестные процессы, подозрительный вход в систему), необходимо начать анализ угроз;
* если анализ показал наличие вредоносного кода или подозрительных изменений в системе, требуется выполнить дополнительную проверку на вирусы;
* если обнаруженная угроза является критической (например, зафиксировано распространение вируса по сети), следует немедленно заблокировать заражённые файлы и отключить заражённый узел;
* если зафиксирована DDoS-атака (высокий объем трафика с подозрительных IP-адресов), система должна активировать механизмы фильтрации;
* если обнаружены попытки взлома паролей или несанкционированный доступ, система должна запросить многофакторную аутентификацию;
* если выявлена уязвимость в программном обеспечении, необходимо уведомить администратора и предложить обновление ПО.

4) Рассмотрим несколько распространённых угроз компьютерной безопасности, которые могут быть учтены в продукционной модели:

1. вирусы и вредоносное ПО
   * распространение через вложения в письмах, вредоносные ссылки, заражённые файлы;
   * может привести к краже данных, потере информации, разрушению файловой системы.
   * требует немедленного выявления и устранения.
2. DDoS-атаки
   * направлены на перегрузку серверов, что может привести к недоступности сервисов;
   * необходима фильтрация трафика и блокировка подозрительных IP-адресов.
3. взлом паролей
   * использование атак перебора паролей (Brute Force) или кража учетных данных;
   * требует принудительной смены пароля и включения многофакторной аутентификации.
4. уязвимости в ПО
   * ошибки в программном обеспечении, которые могут быть использованы злоумышленниками;
   * требуется своевременное обновление и исправление уязвимостей.

5) Вышеописанное можно преобразовать в следующие предложения типа «Если, то»:

* если субъект обнаружил аномальную активность в системе, то субъект должен выполнить анализ угроз;
* если субъект выполнил анализ угроз и выявил наличие вредоносного ПО, то субъект должен провести антивирусную проверку системы;
* если субъект выявил, что вредоносное ПО обладает критическими свойствами, то субъект должен немедленно заблокировать заражённые файлы и изолировать инфицированное устройство;
* если субъект зафиксировал DDoS-атаку, то субъект должен включить механизмы фильтрации сетевого трафика и заблокировать подозрительные IP-адреса;
* если субъект обнаружил подозрительную активность учетной записи, то субъект должен запросить многофакторную аутентификацию у пользователя;
* если субъект выявил уязвимость в программном обеспечении, то субъект должен уведомить администратора и порекомендовать обновление безопасности;
* если субъект устранил угрозу, то субъект должен вернуть систему в нормальный режим работы.

Введем обозначения для фактов (Ф), действий (Д) и продукций (П), тогда:

Субъект = администратор системы или автоматизированная система защиты.

* Ф1 = субъект обнаружил аномальную активность в системе;
* Ф2 = субъект выявил наличие вредоносного ПО;
* Ф3 = субъект установил, что вредоносное ПО критическое (саморазмножается, изменяет системные файлы, передает данные злоумышленникам);
* Ф4 = субъект зафиксировал DDoS-атаку;
* Ф5 = субъект обнаружил подозрительную активность учетной записи;
* Ф6 = субъект выявил уязвимость в программном обеспечении;
* Ф7 = субъект устранил угрозу и может вернуть систему в нормальный режим.
* Д1 = субъект выполняет анализ угроз;
* Д2 = субъект проводит антивирусную проверку системы;
* Д3 = субъект блокирует вредоносное ПО и изолирует заражённые файлы;
* Д4 = субъект активирует фильтрацию сетевого трафика и блокирует подозрительные IP-адреса;
* Д5 = субъект запрашивает многофакторную аутентификацию у пользователя;
* Д6 = субъект уведомляет администратора о необходимости обновления безопасности;
* Д7 = субъект возвращает систему в нормальный режим работы.

Для продукций установим приоритет (в скобках перед запятой, чем выше приоритет, чем раньше проверяется правило).

* П1(4, Ф1) = Д1;
* П2(3, Ф2) = Д2;
* П3(2, Ф3) = Д3;
* П4(2, Ф4) = Д4;
* П5(2, Ф5) = Д5;
* П6(2, Ф6) = Д6;
* П7(1, Д3 или Д4 или Д5 или Д6) = Д7.

6) Для отображения взаимосвязи продукций построим граф (рис. 1).

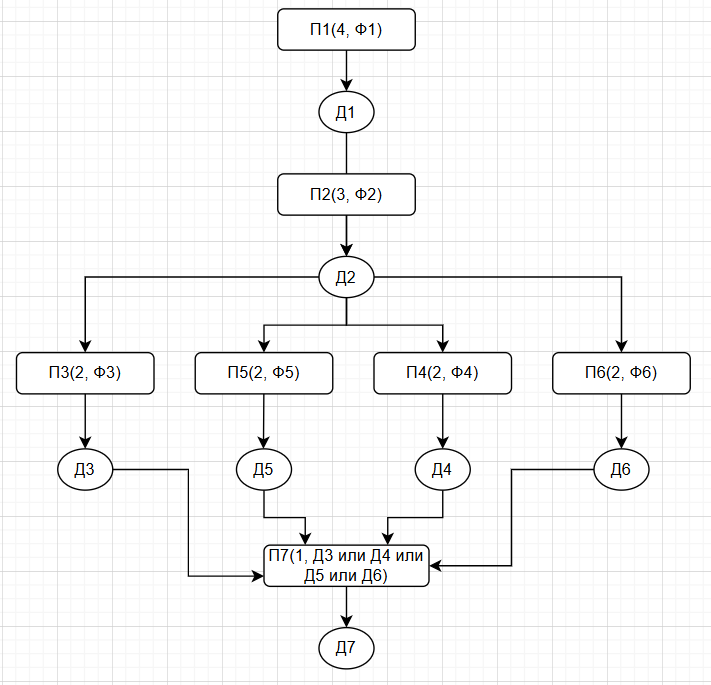


Рисунок – Граф, отображающий взаимосвязи продукций

## Часть 2.

Необходимо заполнить пустую оболочку экспертной системы знаниями из таблицы (рисунок 2).

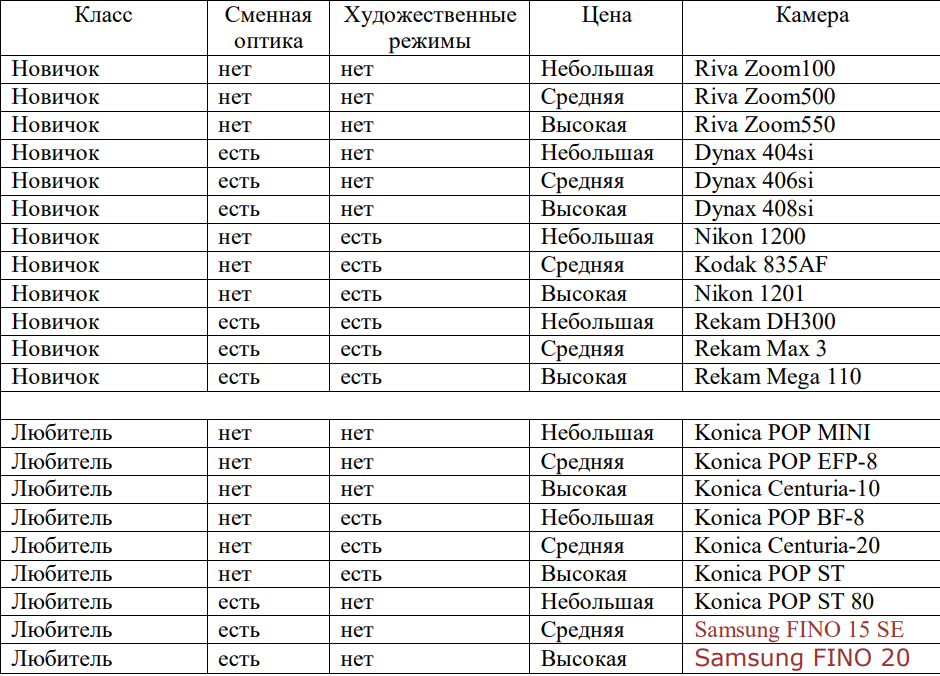




Рисунок – Таблица значений

Пример для любителя, готовым заплатить высокую цену изображен на рисунках 3-8.

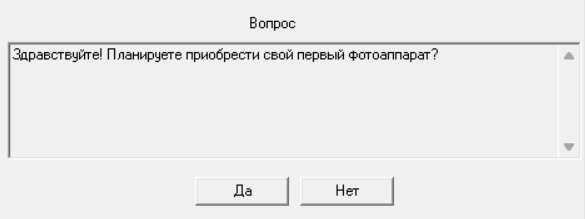


Рисунок – Выбор класса покупателя

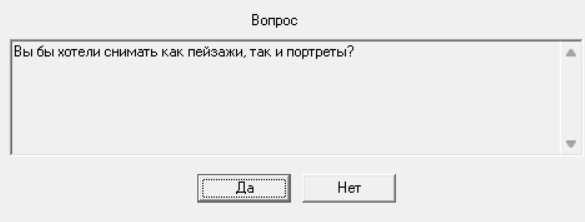


Рисунок – Выбор класса покупателя

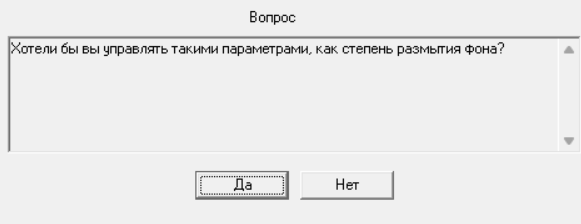


Рисунок – Выбор наличия степени размытия фона

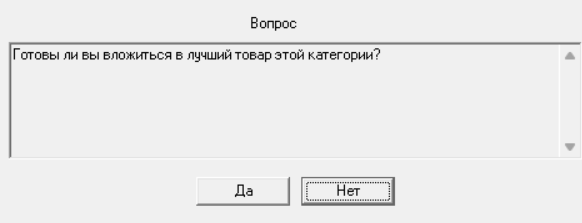


Рисунок 6 – Выбор категории цены

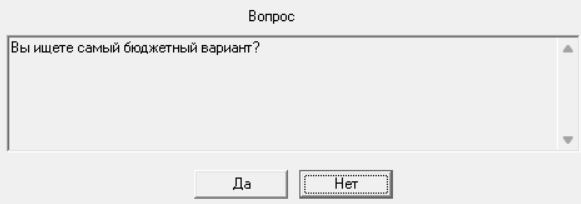


Рисунок 7 – Выбор категории цены

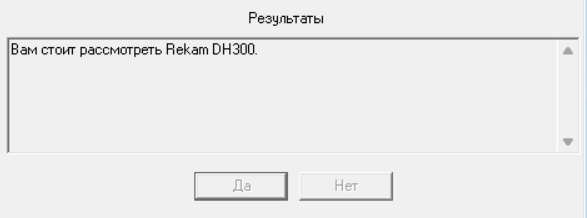


Рисунок 8 – Результат

# **ЗАКЛЮЧЕНИЕ**

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

**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: 25.02.2025). – Режим доступа: для авториз. пользователей. – Текст: электронный.