Попов, М. А., Федоров, Д. Ю. Пример построения онтологии в области защиты информации / М.А. Попов, Д.Ю. Федоров // Защита информации в компьютерных системах / под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. - СПб. : Изд-во СПбГЭУ, 2017. – С. 13-19

Попов М.А., студент 3 курса направления «Информационная безопасность»
Федоров Д. Ю., старший преподаватель кафедры ВСиП

ПРИМЕР ПОСТРОЕНИЯ ОНТОЛОГИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Обеспечение государственно-правового регулирования предполагает опору на формализованную нормативно-правовую базу. Это относится к любой области, в частности, к защите информации. Одним из способов формализации является построение онтологии в области защиты информации. Онтология – это попытка всеобъемлющей и подробной формализации некоторой области знаний с помощью концептуальной схемы. Онтологии используются как форма представления знаний о реальном мире или его части [1].

Онтология может быть использована как источник энциклопедических знаний в области защиты информации, например, гораздо проще «заполнять пробелы» в знаниях или изучать новые области через графическое представление. С ее помощью можно определять, к какой сфере защиты информации относится то или иное понятие. Это может быть полезно, например, для анализа текстов, для проверки актуальности определения (насколько давно введено понятие).

Так как в стандартах описаны, в том числе, процессы обеспечения информационной безопасности, анализ онтологии может позволить проверить правильность существующего процесса или спланировать новый.

Рассмотрим алгоритм формирования (этапы построения) онтологии для области защиты информации.

1. Создается класс, совпадающий с названием нормативного документа (далее – НД).
2. Описание и область применения НД заносятся в комментарий к классу.
3. НД логически разделяются и создаются подклассы.
4. Для подклассов создаются другие подклассы до тех пор, пока полностью не будет раскрыто содержание НД.
5. Определения заносятся в комментарий подкласса.
6. Примечания с определениями заносятся в комментарии.

Изначально был рассмотрен ГОСТ Р-50922-2006, содержащий основные термины, использующиеся в защите информации. В отдельный класс были выделены определения общетехнических понятий. Следующим в онтологию был внесен ГОСТ Р 50.1.053-2005, так как в нем содержатся термины, относящиеся к технической защите информации.

Также в отдельный класс были вынесены иноязычные эквиваленты терминов. Далее был создан подкласс «Методы проведения программных средств на наличие вирусов», в комментарии была занесена основная информация раздела, к этому классу был создан подкласс «Программные методы», к которому были созданы подклассы, перечисляющие методы. Информация о том, чем отличаются программно-аппаратные методы, была занесена в комментарий к классу «Программные методы». Определения программных методов были занесены в комментарии к соответствующим классам.

Затем был создан подкласс «Порядок проведения испытаний программных средств», основные положения пункта были занесены в комментарии. К нему был создан подкласс «Меры по защите проверяемых программных средств», к этому классу были созданы подклассы: «Меры по защите проверяемых программных средств», «Технические средства испытательного стенда», «Обязанности испытательного стенда», «Состав работ по подготовке» и «Проверка программных средств на наличие компьютерных вирусов». Данный ГОСТ очень сильно устарел, было даже несколько неловко заносить информацию о том, например, что информацию необходимо передавать на дискетах. Попытки найти более новую версию ГОСТа успехом не увенчались.

«ГОСТ Р 51275-2006 – Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Первым подклассом были введены «Термины и определения» по аналогии со всеми предыдущими, далее были созданы подклассы «Основные положения» и «Классификация факторов». Основные положения были занесены в комментарии. В классификации основная информация также была в комментариях, но факторы были вынесены в подкласс.

По аналогии в онтологию были внесены ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты», ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения», ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества», ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств», ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». В процессе работы часто было трудно найти определенный стандарт или его переизданную версию.

На рисунке 1 представлен фрагмент онтологии для области защиты информации.

Попов, М. А., Федоров, Д. Ю. Пример построения онтологии в области защиты информации / М.А. Попов, Д.Ю. Федоров // Защита информации в компьютерных системах / под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. - СПб. : Изд-во СПбГЭУ, 2017. – С. 13-19

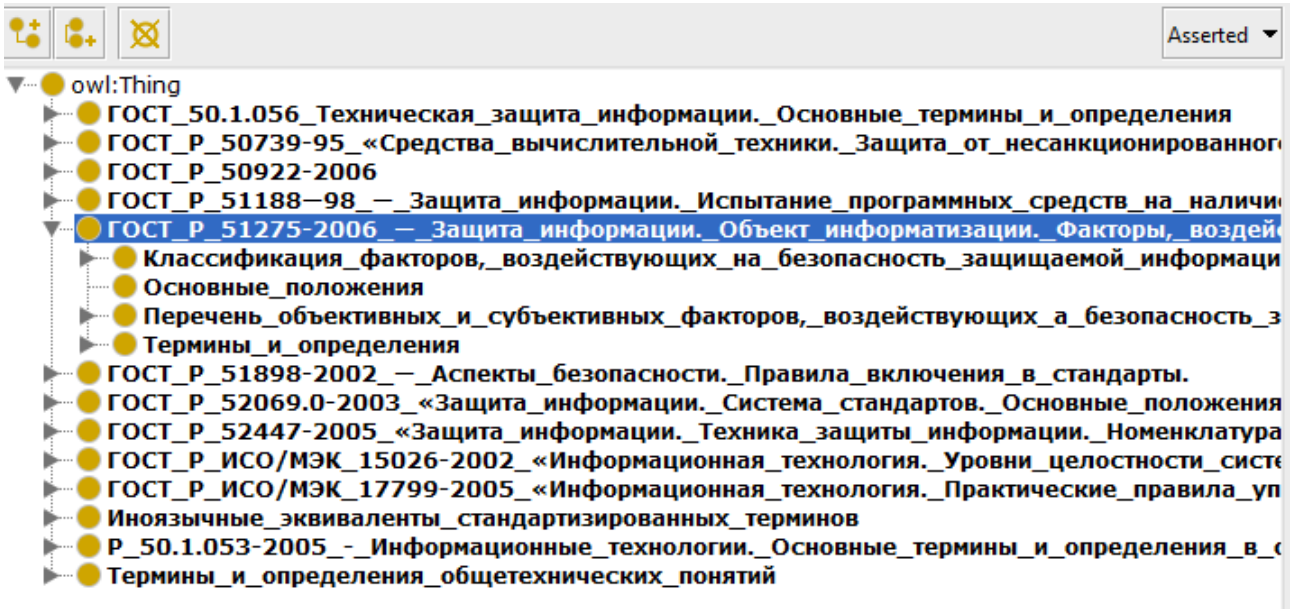

Рис. 1. Фрагмент онтологии для области защиты информации

На рисунке 2 представлен фрагмент визуального представления онтологии для области защиты информации.

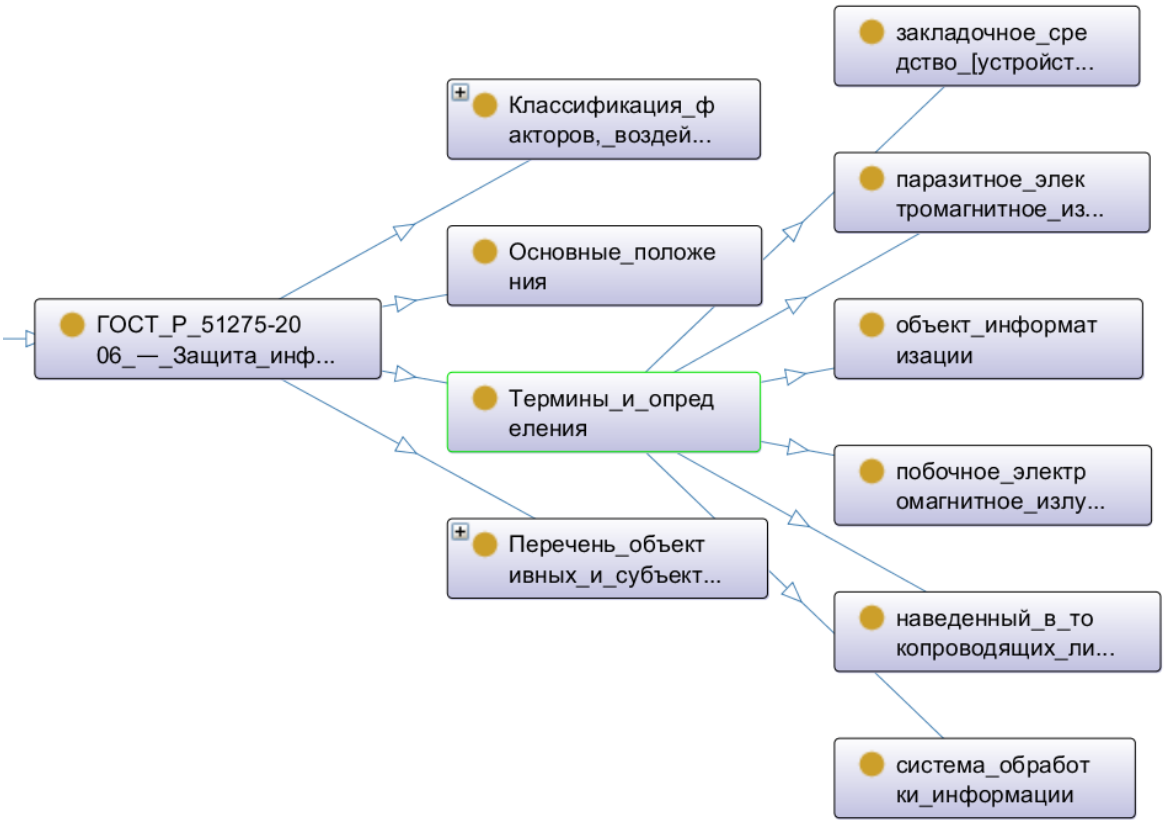

Рис. 2. Фрагмент визуального представления онтологии для области защиты информации

Для демонстрации автоматизированного анализа полученной онтологии был выбран язык Python [2] и модуль Owlready2[1]. В результате была разработана программа, позволяющая через анализ онтологии получить определение термина и соответствующие ему предыдущий и последующий субклассы.

На рисунке 3 представлена блок схема алгоритма работы программы.

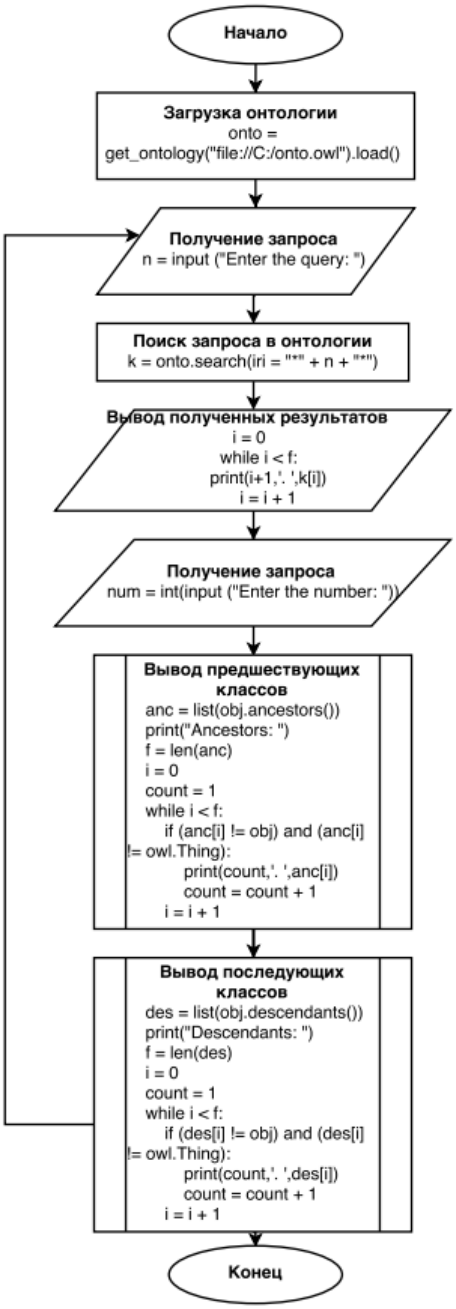

Рис. 3. Блок схема алгоритма работы программы

[1] Полная документация находится по адресу: http://pythonhosted.org/Owlready2/

Попов, М. А., Федоров, Д. Ю. Пример построения онтологии в области защиты информации / М.А. Попов, Д.Ю. Федоров // Защита информации в компьютерных системах / под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. - СПб. : Изд-во СПбГЭУ, 2017. – С. 13-19

Далее представлен исходный текст программы:

```
from owlready2 import*
# Загрузка онтологии
onto = get_ontology("file://C:/onto.owl").load()
while True:
    n = input ("Enter the query: ")
    k = onto.search(iri = "*" + n + "*")
    f = len(k)
    i = 0
    while i < f:
        print(i+1,'. ',k[i])
        i = i + 1
    num = int(input ("Enter the number: "))
    obj = k[num-1]
    if obj.comment:
        print(obj, " - ", obj.comment)
    # предыдущий субкласс:
    anc = list(obj.ancestors())
    print("Ancestors: ")
    f = len(anc)
    i = 0
    count = 1
    while i < f:
        if (anc[i] != obj) and (anc[i] != owl.Thing):
            print(count,'. ',anc[i])
            count = count + 1
        i = i + 1
    # последующий субкласс:
    des = list(obj.descendants())
    print("Descendants: ")
    f = len(des)
    i = 0
    count = 1
    while i < f:
        if (des[i] != obj) and (des[i] != owl.Thing):
            print(count,'. ',des[i])
            count = count + 1
        i = i + 1
```

Рассмотрим интерфейс работы с программой. Сначала необходимо ввести требуемое ключевое слово, после этого происходит поиск и выводятся пронумерованные результаты. Следующим шагом будет выбор номера класса из результатов предыдущего шага, после чего программа выведет комментарий, а также предшествующие и последующие классы. Затем программа запустится заново.

Enter the query: вирус
1 . onto.Компьютерный_вирус
2 .
onto.Порядок_проведения_испытаний_программных_средств_на_наличие_компьютерных_вирусов
3 .
onto.Методы_проведения_испытаний_программных_средств_на_наличие_компьютерных_вирусов
4 . onto.ГОСТ_Р_51188—98_—
_Защита_информации._Испытание_программных_средств_на_наличие_компьютерных_вирусов._Типовое_руководство.
5 .
onto.Состав_работ_по_подготовке_к_проведению_испытаний_программных_средств_на_наличие_компьютерных_вирусов
6 . onto.оценку_эффективности_применяемых_антивирусных_средств;
7 . onto.поиск_вирусоподобных_фрагментов_кодов_ПС;
Enter the number: 1
onto.Компьютерный_вирус - ['программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.']
Ancestors:
1 . onto.Определения_и_сокращения
2 . onto.ГОСТ_Р_51188—98_—
_Защита_информации._Испытание_программных_средств_на_наличие_компьютерных_вирусов._Типовое_руководство.
Descendants:
Enter the query:

В результате проделанной работы была создана онтология и осуществлен ее программный анализ. Дальнейшие исследования могут быть направлены на уточнение терминов и добавление нормативных документов.

Библиографический список

1. Гаврилова Т. А., Кудрявцев Д. В., Муромцев Д. И. Инженерия знаний. Модели и методы: Учебник. – СПб.: Издательство «Лань», 2016. – 324 с.
2. Федоров, Д. Ю. Программирование на языке высокого уровня Python : учеб. пособие для прикладного бакалавриата / Д. Ю. Федоров. – М. : Издательство Юрайт, 2017. – 126 с.