Федоров Д. Ю. Подход к комплектации учебно-лабораторной базы программно-аппаратной защиты на основе сетей знаний // Информационное противодействие угрозам терроризма: науч.-практ. журн. – 2015. – Т.1, №25. – С. 384-388

УДК 37.02; 65.011.56

Д.Ю. Федоров
Россия, г. Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПОДХОД К КОМПЛЕКТАЦИИ УЧЕБНО-ЛАБОРАТОРНОЙ БАЗЫ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ НА ОСНОВЕ СЕТЕЙ ЗНАНИЙ

Рассматривается подход к формированию перечня программного и аппаратного обеспечения для учебно-лабораторной базы, основанный на сетях знаний. Излагаются базовые положения теории сетей знаний. Даются определения и аксиоматика автоматизированного процесса обучения. Приводится пример из программы подготовки специалистов по информационной безопасности.

терминология; сеть знаний; автоматизация обучения.

В соответствии с федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 090900 (10.03.01) «Информационная безопасность» для реализации основной образовательной программы требуется наличие лаборатории программно-аппаратных средств обеспечения информационной безопасности.

Существует несколько подходов к формированию перечня программного и аппаратного обеспечения для учебно-лабораторной базы. Один из них – опираться только на популярные продукты в области защиты информации. Другой подход был реализован на кафедре вычислительных систем и программирования СПбГЭУ и базируется на потребностях в обеспечении лабораторных и практических работ конкретной учебной дисциплины. В основу данного подхода была положена модель образовательного процесса, основанная на теории сетей знаний, предложенной проф. В.Я. Розенбергом [1]. Рассмотрим базовые положения данной теории.

Совокупность знаний Θ изучаемой учебной дисциплины представляет собой систему. Элементарной составляющей, входящей в состав Θ является слово (термин), отражающее определенное понятие. С помощью слов фиксируются все понятия, составляющие систему Θ. Связи между понятиями устанавливаются с помощью грамматических правил конкретного языка. По отношению к каждому понятию из Θ существует первичное предложение, которое содержит его определение. Совокупность таких определений образует инвариантное ядро Θ, которое обеспечивает однозначность восприятия знаний в пределах конкретной учебной дисциплины. Инвариантное ядро учебной дисциплины для определения своих понятий использует слова из других областей знаний. Все понятия из Θ делятся на основные и вспомогательные. К основным понятиям относятся специфические понятия данной конкретной дисциплины, являющиеся предметом ее определения и изучения. К вспомогательным понятиям относятся понятия, заимствованные из других областей знаний, которые в данной дисциплине не изучаются, а используются для определения содержания основных понятий. Множество основных понятий конкретной дисциплины, вместе с внутренними взаимосвязями между ними, образует иерархически упорядоченную сеть знаний, узлами которой являются идентификаторы основных понятий [2].

Дадим ряд определений.

Определение 1. Под знанием будем понимать набор терминов, обозначающих понятия, и связи между ними.

Определение 2. Сеть знаний будем называть нормализованной при выполнении двух условий.

Условие 1. Отсутствие в сети знаний рекурсий, т.е. логически противоречивых определений.

Примером нарушения условия являются определения терминов «правила разграничения доступа» и «субъект доступа», представленные в Руководящем документе «Защита от несанкционированного доступа к информации. Термины и определения» [3].

Правила разграничения доступа − совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа − лицо или процесс, действия которого регламентируются правилами разграничения доступа.

В определении термина «правила разграничения доступа» присутствует термин «субъект доступа», а в определении термина «субъект доступа» − термин «правила разграничения доступа». Налицо рекурсия.

Условие 2. Отсутствие в сети знаний, так называемых, «висящих» терминов, т.е. таких, в состав которых не входят термины из области данной дисциплины.

Примером нарушения данного условия являются следующие термины из вышеупомянутого Руководящего документа: «целостность информации», «верификация», «средство криптографической защиты информации», «сертификация уровня защиты».

Введем аксиомы.

Аксиома 1 (о единственности): для заданной учебной дисциплины существует единственная нормализованная сеть знаний.

Утверждает об однозначности представления учебной дисциплины в системе предметных знаний.

Аксиома 2. Образовательный процесс является продвижением по нормализованной сети знаний, т.е. изучением терминов и связей между ними.

Траекторию движения выбирает преподаватель.

Аксиома 3. Необходимым условием изучения основного термина является освоение всех вспомогательных терминов для данного основного термина.

Накладывает условие на предварительные знания учащихся.

Аксиома 4. Достаточным условием освоения дисциплины является изучение всех терминов сети знаний данной дисциплины.

Таким образом, начальным условием осуществления образовательного процесса по заданной дисциплине является наличие ее нормализованной сети знаний. Из аксиомы о единственности следует, что такая сеть знаний существует. В этом случае, формы проведения учебных занятий примут следующий вид. Лекционное занятие служит для изучения очередного понятия из сети знаний дисциплины. На лабораторной работе учащийся ищет новые причинно-следственные связи между понятиями, последующее объяснение которых состоится на лекции. На практическом занятии учащийся эмпирически проверяет наличие связей между понятиями, декларированных на лекции.

В качестве примера рассмотрим термины «машинный код», «язык ассемблера», «ассемблер», «дизассемблер» и «отладчик», которые изучаются в СПбГЭУ бакалаврами информационной безопасности в рамках учебной дисциплины «Про-

граммно-аппаратные средства защиты информации». Данные термины имеют следующие определения:

Машинный код − система команд (набор кодов операций) конкретной вычислительной машины, которая интерпретируется непосредственно процессором или микропрограммами этой вычислительной машины [4].

Язык ассемблера − машинно-ориентированный язык низкого уровня с командами, обычно соответствующими *командам машины*, который может обеспечить дополнительные возможности вроде макрокоманд [5].

Ассемблер − компьютерная программа, компилятор исходного текста программы, написанной на *языке ассемблера*, в программу на *машинном языке* [6].

Дизассемблер − транслятор, преобразующий *машинный код*, объектный файл или библиотечные модули в текст программы на *языке ассемблера* [7].

Отладчик − компьютерная программа, предназначенная для поиска ошибок в других программах, ядрах операционных систем, SQL-запросах и других видах *программного кода* [8]. Включает встроенный *дизассемблер*.

Фрагмент сети знаний для перечисленных выше терминов будет иметь вид, представленный на рисунке 1.

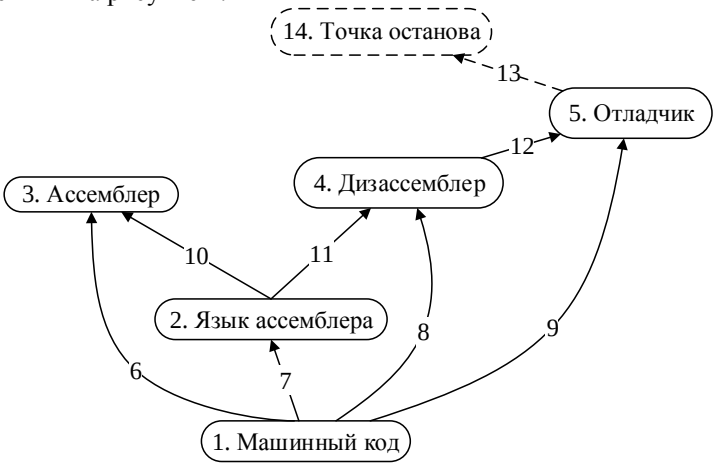

Рис. №1 Фрагмент сети знаний дисциплины «Программно-аппаратные средства защиты информации»

На лекции последовательно, начиная с более низкого уровня, раскрываются термины «машинный код», «язык ассемблера», «ассемблер», «дизассемблер», «отладчик». На практическом занятии под руководством преподавателя учащиеся «в живую» знакомятся с преобразованием машинного кода в код на языке ассемблера, т.е. эмпирически проверяют связи под номерами 6, 7 и 10. Лабораторная работа включает самостоятельное исследование связей термина «отладчик» (9, 12) и выявление его «новых» связей (13) − с неким явлением под номером 14. Впоследствии на лекции будет введено и всесторонне раскрыт термин «точка останова» [9].

Таким образом, наличие сети знаний позволяет разрабатывать лабораторные и практические работы, исходя из понятий изучаемой дисциплины и связей между ними. Это, в свою очередь, задает перечень требований к программному и аппаратному обеспечению для учебно-лабораторной базы. К примеру, понятия и связи, рассмотренные на рисунке 1, могут быть изучены с помощью одного из трех программных продуктов: GDB [10], OllyDbg [11] или IDA Pro [12]. Следую-

щим критерием отбора уже может стать распространенность, стоимость каждого из них.

Сложность подхода к комплектации учебно-лабораторной базы на основе сетей знаний заключается в трудоемкости ручного построения сети. Решением этой проблемы может стать частичная автоматизация. С помощью платформы MediaWiki [13] автоматизируем процесс установления связей [14] между терминами, рассмотренными ранее: «точка останова», «дизассемблер», «ассемблер», «машинный код», «язык ассемблера», «отладчик». После этого напишем на языке программирования Java скрипт, который позволит преобразовать связи между терминами, хранящимися в базе данных MediaWiki, в квадратичную матрицу *M*, где 1 означает, что связь между терминами существует, 0 – связь отсутствует:

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Полученную матрицу подадим на вход системы компьютерной алгебры Wolfram Mathematica [15], где есть возможность визуализировать матрицу, представив ее в виде направленного графа. Таким образом, получим сеть знаний, изображенную на рисунке 2.

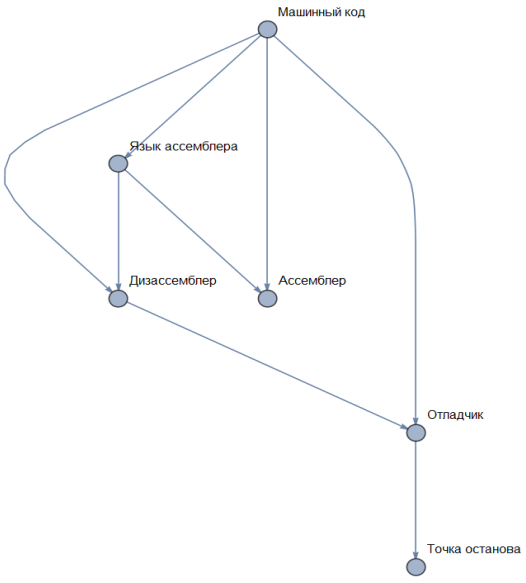

Рис. №2. Фрагмент сети знаний дисциплины «Программно-аппаратные средства защиты информации», построенный в программе Wolfram Mathematica

Предложенный подход может быть аппроксимирован и на другие учебно-лабораторные базы. Необходимым условием в этом случае является наличие нормализованной сети знаний.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Розенберг В. Я.* Система обучения на базе семантических сетей. Теория и практика // Матер. Междунар. научно-практ. конф. «Фундаментальные и прикладные исследования в современном мире», 13-15 марта 2013 г.- СПб.: Информационный издательский учебно-научный центр «Стратегия будущего», 2013. - С. 184–191.

2. *Волынец Ю.Ф.* Теоретические основы формализованного представления педагогических знаний в инфологической среде подготовки специалистов ВМФ./ Под ред. В.Я. Розенберга.− Петродворец: ВМИРЭ, 2000.− 82 с.

3. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»/ Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

4. Машинный код. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Машинный_код (дата обращения 13.04.2015).

5. Язык ассемблера. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Язык_ассемблера (дата обращения 13.04.2015).

6. Ассемблер. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Ассемблер (дата обращения 13.04.2015).

7. Дизассемблер. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Дизассемблер (дата обращения 13.04.2015).

8. Отладчик. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Отладчик (дата обращения 13.04.2015).

9. Точка останова. Статья в Википедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Точка_останова (дата обращения 13.04.2015).

10. Официальный сайт программы The GNU Project Debugger [Электронный ресурс]. – Режим доступа: https://www.gnu.org/software/gdb/ (Дата обращения 12.04.2015).

11. Официальный сайт программы OllyDbg [Электронный ресурс]. – Режим доступа: http://www.ollydbg.de (Дата обращения 12.04.2015).

12. Официальный сайт программы IDA Pro [Электронный ресурс]. – Режим доступа: https://www.hex-rays.com (Дата обращения 12.04.2015).

13. Официальный сайт программы MediaWiki [Электронный ресурс]. – Режим доступа: https://www.mediawiki.org/wiki/MediaWiki (Дата обращения 12.04.2015).

14. База знаний информационной безопасности [Электронный ресурс]. – Режим доступа: http://wiki.dfedorov.spb.ru/wiki/index.php?title=Категория:Анализ_кода_программы (Дата обращения 13.04.2015).

15. Официальный сайт программы Wolfram Mathematica [Электронный ресурс]. – Режим доступа: http://www.wolfram.com/mathematica/ (Дата обращения 13.04.2015).