5 Підготовка, перепідготовка та підвищення кваліфікації спеціалістів систем захисту інформації

УДК 681.39:371

ИНТЕЛЛЕКТУАЛИЗАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБУЧЕНИЯ, ОРИЕНТИРОВАННЫХ НА ПОДГОТОВКУ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Владимир Тарасенко, Антон Михайлюк, Юрий Балицкий
Национальный технический университет Украины «КПИ»

Анотація: **Пропонуються оригінальні шляхи інтелектуалізації автоматизованих навчальних систем, що зорієнтовані на підготовку спеціалістів у галузі захисту інформації.**

Summary: **In this article proposed some original ways to intellectualization automatic learning systems, which are oriented to information defence specialists training.**

Ключові слова: **Автоматизовані навчальні системи, захист інформації, інтелектуалізація.**

Необходимость обучения и повышения квалификации специалистов в области защиты информации в XXI веке не вызывает сомнений. В связи с растущими темпами информатизации общества потребность в специалистах в данной области постоянно увеличивается. Наиболее перспективное решение – это внедрение автоматизированных способов обучения и контроля знаний. Автоматизированные системы обучения (АСО) можно использовать как при стационарном обучении, так и при дистанционном.

Рассмотрим поэтапно процесс работы специалиста в области защиты информации и на основе этого сформулируем требования к автоматизированной системе.

Прежде всего, имеется некоторый объект, который необходимо защитить от несанкционированного доступа к информации. В роли такого объекта может выступать как отдельный компьютер, комната или компьютерный класс, так и некоторое множество помещений, целое здание. Многообразие объектов защиты вносит дополнительные сложности в процесс работы специалиста, поскольку требует навыков для работы с каждой разновидностью таких объектов.

Начальный этап – получение характеристик объекта защиты. Если объект является достаточно простым (скажем, один компьютер), достаточно просто иметь набор технических характеристик. В случае наличия сложного объекта или системы объектов необходимо, с одной стороны, наличие множества технических характеристик, а с другой стороны – непосредственный осмотр специалистом объекта. Если речь идет, например, о защите некоторой комнаты с несколькими терминалами, то осмотр является необходимостью. Кроме того, при осмотре объекта специалист должен иметь возможность получать дополнительную информацию, поэтому можно говорить о необходимости сопровождения со стороны организации-заказчика.

Второй этап – анализ полученной информации. Проводится непосредственно экспертом в области защиты информации. Основная цель анализа – оценить текущее состояние объекта с точки зрения защиты информации и сформулировать некоторую стратегию защиты.

Третий этап – выработка рекомендаций. Проводится на основе выбранной стратегии и зачастую имеет комплексный характер.

Автоматизированная система обучения должна обеспечить прохождение вышеописанных этапов и проконтролировать правильность сделанных выводов. Сформулируем требования к АСО.

1. Система должна продемонстрировать защищаемый объект, либо представить достаточно полное описание. Для этого необходимо создание некоторой базы данных (БД), из которой будет выбираться объект для текущей задачи.
2. Если реализована демонстрация объекта, то система должна позволять получать дополнительную информацию на этапе осмотра.
3. В зависимости от этапа обучения необходимо обеспечить помощь в анализе объекта.
4. Наличие возможности ввода конечных рекомендаций для защиты объекта.
5. Наличие проверки результатов и выставление оценки.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Требования 3, 4 являются стандартными для любой системы обучения, поэтому не будем на них останавливаться.

Рассмотрим требования 1 и 2. Здесь можно выделить три основные проблемы:

1) проблема базы данных объектов;
2) проблема демонстрации объекта обучаемому;
3) проблема выдачи характеристик объекта и дополнительной уточняющей информации.

Традиционный подход к удовлетворению этих требований и решению трех проблем следующий. Создается некоторая база данных возможных объектов. Базу данных составляют эксперты, они же анализируют и заносят возможные варианты защиты этих объектов. Объекты в базе данных группируются по сложности, образуя несколько уровней. В зависимости от текущего уровня обучаемого система просто выбирает готовый объект. Демонстрация проводится с помощью заложенных в БД фотографий (либо вообще не проводится, а выдается только список характеристик). Возможности получения дополнительной информации ограничены объемом, вложенным в БД. По мере эксплуатации в систему могут добавляться новые объекты или заменяться старые.

Предлагается принципиально новый подход к решению вышеперечисленных трех проблем.

Для демонстрации защищаемого объекта можно использовать технологию трехмерного моделирования. Создание аппаратных и программных средств моделирования трехмерных объектов – одно из перспективных направлений развития компьютерной техники. Концепция «виртуального мира» применяется в самых различных областях. Для создания достоверного «виртуального пространства» необходимы следующие составляющие:

1) пакет моделирования трехмерных объектов;
2) готовые модели, полученные с помощь этого пакета;
3) система визуализации, задача которой – отрисовывать видимое пространство с объектами, в зависимости от координат и направления вектора «виртуальной камеры»;
4) система контроля столкновений, не позволяющая передвигаться сквозь стены и другие препятствия;
5) система управления передвижением, задача которой – изменять координаты и направление вектора «виртуальной камеры» в зависимости от управляющих воздействий пользователя.

Таким образом, имея систему визуализации со встроенными системами управления и контроля столкновений и имея трехмерную модель исследуемого объекта, можно создать для субъекта иллюзию передвижения по «виртуальному пространству». При этом пользователь будет иметь возможность подробно осмотреть исследуемый объект, скажем, комнату с офисной мебелью, компьютерной техникой, окнами и т. д. Такой подход обеспечивает значительно более высокий уровень наглядности и позволяет получить более полное впечатление, чем при просмотре описания комнаты: ее размеров, координат расположения офисной техники внутри и т. д.

Следующий шаг – реализация технологии «коснись-и-узнаешь». Суть этой технологии в том, что, находясь в «виртуальном помещении», пользователь имеет возможность узнавать характеристики различных объектов, касаясь их, скажем, с помощью некоторого указателя. При этом необходимо организовать некоторую систему иерархии: показав на составной объект можно узнать его общие характеристики и состав; показав на какую-то часть – получить информацию конкретно про эту часть.

Вместе это должно заменять этап получения характеристик при работе эксперта на конкретном объекте. Пользователь будет иметь возможность выяснить все интересующие детали относительно исследуемого объекта так же, как и в реальном мире – спросив про него. У такого подхода есть существенное отличие от ситуации, когда обучаемый получает в руки распечатку со всеми необходимыми параметрами и характеристиками. Теперь обучаемый должен сам указывать, какая информация ему нужна для проведения анализа. И, в случае, если он не обладает достаточными знаниями и навыками, его действия будут ближе к реальности, где необходимо самостоятельно запрашивать информацию, а не получать ее в готовом виде. В общем, этап сбора информации – это тоже часть работы эксперта и необходимо сделать этот этап максимально реалистичным, что и достигается с помощью «виртуального мира» и технологии «коснись-и-узнаешь».

Вернемся к этапу заполнения БД системы моделями объектов для учебных задач и к требованию организации проверки введенных рекомендаций и выставлению оценки.

Существенный недостаток описанного подхода – большой объем работы для заполнения базы данных. Эта работа требует совместной работы дизайнеров и экспертов в области защиты информации и основной ее недостаток – ограниченное количество объектов в БД. Создание достаточно большого количества объектов для того, чтобы в процессе обучения они не повторялись – чрезмерно трудоемкое занятие, поскольку кроме трехмерного моделирования требуется еще и проведение всех необходимых расчетов и выводов для каждого

объекта в отдельности. Кроме того, требуется хорошее воображение для того, чтобы нарисовать, предположим, несколько сотен офисных комнат или несколько десятков разных зданий с различными конфигурациями.

Решается это путем отказа от БД объектов и использования алгоритмов динамической генерации объектов определенных классов с заданными характеристиками и экспертной системы для оценки защищенности объекта.

Рассмотрим, для примера, в общих чертах, механизм генерации «виртуального офиса».

1. Имеется некоторый набор правил, которые справедливы для генерируемого объекта, например:

a) офис состоит из нескольких комнат;
b) площадь каждой комнаты не меньше 10 кв. метров;
c) соотношение длины и ширины от 1:1 до 2,5:1;
d) высота потолка от 2,4 до 4 метров;
e) каждая комната должна иметь вход и т.д.

2. В соответствии с этими правилами псевдослучайно генерируются параметры комнат.
3. Выбираются текстуры для пола, стен, потолка, дверей. Создать библиотеку текстур для стен в количестве 20 достаточно просто.
4. Расставляется офисная мебель по своему набору правил. Образцы мебели также хранятся в библиотеке.
5. Генерируются компьютеры. Известно, что компьютер состоит из системного блока, монитора, клавиатуры и т.д. Образцы каждой детали в нескольких вариантах хранятся в библиотеке. Псевдослучайно выбирая каждую деталь из 5-6 хранимых вариантов, в итоге можно получить достаточно много сборных моделей компьютеров.
6. Генерируются все остальные объекты в комнате.
7. Определяются разнообразные характеристики и параметры .
8. Расставляются существующие средства защиты информации.

С таким подходом в библиотеке достаточно хранить только несколько вариантов каждой детали интерьера. Очевидно, что готовые, цельные комнаты никогда не повторятся.

При каждом сеансе работы будет создаваться свой набор комнат, каждая со своим интерьером и характеристиками. Передвигаясь по «виртуальным помещениям», обучаемый узнает всю необходимую информацию по принципу «коснись-и-узнаешь». По истечению некоторого времени или по желанию пользователя, система переходит в режим ввода ответов и рекомендаций. Это может быть реализовано несколькими вариантами.

1. Система переключается в диалоговый режим, и дальнейшая работа ведется в нем.
2. Система остается в режиме «виртуального мира», только теперь пользователь имеет возможность расставлять по комнатам устройства защиты, передвигать мебель и т.д. Устройства защиты выбираются из некоторой «палитры», параметры каждого устройства известны. Указав место, можно закрепить на него прибор.

Последний этап – работа экспертной системы, которая оценивает уровень защищенности, созданный пользователем, подсчитывает ориентировочную стоимость «проведенных работ» и делает выводы о квалификации обучаемого. Экспертная система получит в качестве входной информации параметры защищаемого объекта с «учтенными» рекомендациями и первая ее задача – вычислить индекс защищенности, который будет в процентах выражать степень защищенности. Вторая задача – оценить, является ли достаточным «достигнутый» индекс защиты для текущего уровня обучаемого и в зависимости от результата – выставить оценку.

Создание подобных систем, безусловно, задача не простая, но качество обучения при этом поднимется на новый уровень.

Следует также отметить, что подобный подход можно использовать не только в области защиты информации, но и в большинстве других областей. Так на кафедре специализированных компьютерных систем Национального технического университета Украины «Киевский политехнический институт» уже длительное время ведутся работы в двух направлениях: создание экспертных систем для оценки защищенности объектов и разработка рекламно-информационных систем типа «виртуальный мир». Результаты работ свидетельствуют о больших перспективах предложенного подхода.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.