УДК 378

РАЗРАБОТКА ОБРАЗОВАТЕЛЬНОЙ ТЕХНОЛОГИИ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гавриленко П. В., Котляр Е. В., Тахтуева К. В.

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, Красноярск (660014 г. Красноярск, проспект имени газеты «Красноярский рабочий», 31)

Основной целью данной работы является повышение эффективности обучения специалистов в области информационной безопасности путем использования в процессе обучения компьютерных моделей, основанных на методе имитационного моделирования. В работе обозначены некоторые проблемы обучения специалистов в области информационной безопасности и возможные пути их решения методами имитационного моделирования. Проведен анализ некоторых существующих методов моделирования процесса обеспечения информационной безопасности. Предложена методика моделирования объекта защиты с позиции управления информационной безопасностью, основанная на разделении и учете списка факторов, негативно влияющих на безопасность информации. Сформированы требования к модели, на основании которых разработана образовательная технология моделирования процесса обеспечения информационной безопасности. Предложена методика обучения с помощью разработанного программного комплекса в режиме практических занятий и лабораторных работ. Описаны перспективы внедрения и развития предложенной технологии.

Ключевые слова: имитационное моделирование, управление информационной безопасностью, образовательные технологии.

DEVELOPMENT OF EDUCATIONAL TECHNOLOGY BASED ON SIMULATION MODELLING OF THE INFORMATION SECURITY MANAGEMENT

Gavrilenko P. V., Kotlyar E. V., Tahtueva K. V.

Siberian State Aerospace University, Krasnoyarsk (660014 Krasnoyarsk, Krasnoyarskiy rabochiy, 31)

The main purpose of this work is the improving of the training of specialists in the field of information security through the use of the learning process of computer models based on the method of simulation. This work identifies some problems of training specialists in the field of information security and offers possible methods of their solution based on simulation modeling. An analysis of some existing methods of modeling the process of information security. Method is proposed for modeling the object of protection from a position of information security management based on the differentiation, and registration the list of factors that negatively affect the security of information. Formed to the requirements of the model on which to develop educational process modeling technology of information security management in a mode of practical exercises and laboratory work. Described the prospects for implementation and development of the proposed technology.

Keywords: simulation modeling, information security management.

Современная педагогика ставит перед собой ряд задач, одной из которых является создание универсальных программ обучения специалистов. Наличие таких программ и автоматизированных средств обучения позволяет решать множество проблем, связанных с обучением специалистов в различных областях. Моделирование проблемных ситуаций для последующего их разрешения значительно экономит время и ресурсы, связанные с обучением специалистов. Несомненным плюсом таких методик является возможность обучаемого приобретать навыки, близкие к практическим, что повышает качество знаний выпускников и дает возможность использовать полученный опыт в рамках своей профессиональной деятельности. Метод моделирования, широко применяющийся в рамках инженерной психологии, решает основную задачу, связанную с уменьшением количества

ошибок человека-оператора в ходе эксплуатации управляемых им объектов. Суть данного метода заключается в моделировании управляемого объекта и вариантов воздействия на него, поэтому его можно применять для обучения специалистов, чья профессиональная деятельность впоследствии будет связана с принятием управленческих решений.

Одной из специальностей, где необходим навык формирования комплекса мер воздействия на управляемый объект, является обеспечение информационной безопасности [7]. Эта область знаний сейчас является актуальной, но методики обучения с помощью моделирования реального объекта к ней практически не применяются. Стоит отметить, что на сегодняшний день для развития и проверки навыков специалистов по защите информации, как в процессе профессиональной деятельности, так и в процессе обучения, применяется множество различных методик. В большинстве своем они заключаются в изучении требований стандартов по защите информации, базовых элементов автоматизированных систем (АС) и способов их взаимодействия с помощью вспомогательных средств – систем поддержки принятия решений [1-3 и др.]. Данные методы не могут в полной мере развить навыки, необходимые для профессиональной деятельности специалиста. Как уже отмечалось ранее, одним из способов развития таких навыков является моделирование объекта защиты, оценка негативного влияния на информацию, подлежащую защите на данном объекте, и выработка эффективных комплексных решений по нейтрализации данного влияния. Проблема данного метода заключается в сложности моделирования “поведения” АС и оценки влияния как негативных факторов, так и методов воздействий на них. Поэтому разработка образовательной технологии, которая могла бы моделировать данные процессы, является актуальной на данный момент проблемой, т.к. она может существенно повысить эффективность обучения специалистов в сфере информационной безопасности, а навыки, приобретенные в процессе использования данного программного обеспечения, будут гораздо ближе к практическим, чем при традиционных методах обучения.

Несмотря на сложность моделирования автоматизированной системы как объекта защиты информации, на данный момент уже существуют программные средства и методики моделирования, связанные с процессом обеспечения безопасности информации, поэтому перед разработкой модели целесообразно будет рассмотреть имеющиеся на данный момент подходы.

Методика Домарева

В. В. Домарев разработал свою модель оценки систем ЗИ, основанную на системном подходе [4]. Понятие системности, по Домареву, заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех

этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый целостный механизм – систему защиты.

Создавая данную модель, Домарев исходил из того, что многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том, как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно, чтобы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые требования специалистов по обеспечению информационной безопасности.

Практическая задача обеспечения информационной безопасности состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС. В упрощенном виде модель СЗИ представлена на рисунке 1.

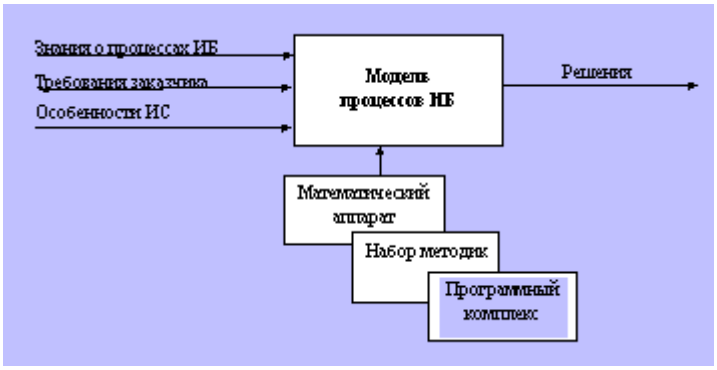

Рисунок 1. Упрощенная модель СЗИ

Основной задачей моделирования является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Digital Security Office 2006 – законченное решение для комплексного управления информационной безопасностью компании. **Digital Security Office 2006** включает в себя систему анализа и управления информационными рисками **ГРИФ** и систему разработки и управления политикой безопасности информационной системы **КОНДОР**. С помощью программы **КОНДОР** проводится аудит ИС компании на соответствие стандарту ISO 17799.

На основе данных, полученных в результате проведения аудита, разрабатывается политика безопасности компании и система управления информационной безопасностью [8].

Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE) [9]

OCTAVE – это метод выявления и оценки угроз, уязвимостей, рисков и мер по их устранению на предприятии. Метод основан на ряде критериев, которые определяют основные источники рисков для самостоятельной их оценки и принятия мер по их устранению. Несмотря на то, что это метод самостоятельной оценки безопасности информационных технологий, он также допускает использование экспертов для проведения конкретных мероприятий, в случае необходимости. OCTAVE представляет собой набор документов с руководством по внедрению данного метода. Руководство состоит из 18 частей и включает в себя: подробное описание метода, рекомендации по подбору и подготовке персонала, руководство по оценке и рисков, и методов их устранения, описание всевозможных информационных потоков на предприятии.

OCTAVE-метод использует трехэтапный подход для рассмотрения организационных и технологических вопросов защиты ИБ, создавая полную картину ИБ организации и её потребностей. При использовании данного метода используются семинары и приветствуется открытое обсуждение и обмен информацией об угрозах, совместная выработка стратегии их устранения. Каждый этап состоит из нескольких процессов, каждый процесс включает в себя один или несколько рабочих совещаний, проводимых группой аналитиков.

Рассмотренные подходы к моделированию АС и процесса обеспечения информационной безопасности разрабатывались с целью выявления угроз безопасности информации в АС, оценки рисков и выработки методов нейтрализации этих угроз. Однако основной целью данной работы является моделирование непосредственно самого процесса защиты информации. Т.е. формирование неких событий, негативно влияющих на защищенность информации в АС, предложение пользователю возможных решений по нейтрализации данного воздействия и оценки выработанного им решения. Одним из методов, которые можно использовать для моделирования объекта защиты, является метод, предложенный в статье В. В. Золотарева, Е. А. Даниловой [5]. Этот метод предполагает разбиение АС на следующие структурные элементы: ОМ – организационные меры защиты информации, ТС – технические средства, ПО – программное обеспечение, Ч – человеческий фактор. Также предполагается, что каждый элемент системы может находиться в одном из следующих состояний: Отк – отказ, О – ошибка, С – сбой, Р – работоспособное состояние. Все подсистемы и состояние представляются в виде матрицы (рис.1), в которой впоследствии исключаются невозможные либо не влияющие на защищенность информации состояния.

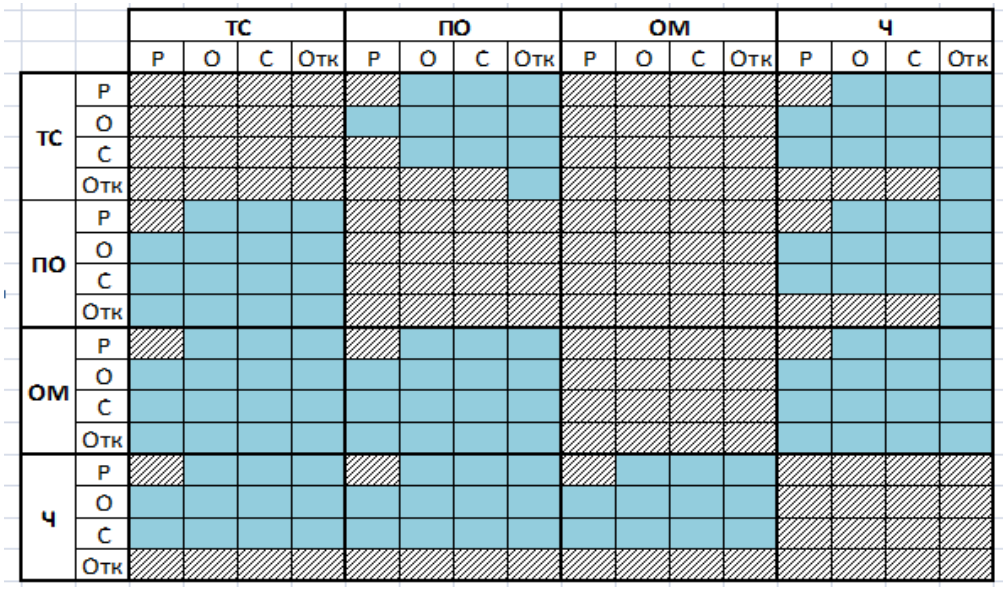

Рисунок 1. Матричное представление декомпозиции факторов

Данная матрица отражает взаимодействие различных элементов системы в зависимости от их состояний, но сами состояния заданы в общем виде (например, рассматривается взаимодействие любого ПО с любыми ТС), поэтому для увеличения комбинаций этих состояний можно разделить (конкретизировать) предложенные элементы системы (ПО, ТС, МО и Ч) и рассмотреть их взаимодействие. Это существенно расширит количество состояний и вариантов их взаимодействия и поможет исключить некоторые невозможные взаимосвязи. В рамках поставленной задачи было принято следующее деление.

Организационные меры:

- меры, направленные на сотрудников организации (включают в себя подбор, проверку, инструктаж сотрудников);
- меры, направленные на защиту информации от лиц, не являющихся сотрудниками организации, но имеющих потенциальную возможность нанести вред защищаемой информации (напр., обеспечению режима физической охраны объектов).

Человеческий фактор:

- персонал, работающий с защищаемой информацией (напр., бухгалтера, директор);
- персонал, обеспечивающий защищенность информации (напр., системный администратор, охранники).

Данное деление выбрано с учетом мер, которые специалист по защите информации может применять к той или иной группе персонала в процессе деятельности. Т.е. по отношению к персоналу, работающему с защищаемой информацией, список мер ограничивается инструктажем и проверкой их деятельности, в то время как меры по отношению ко второй

группе персонала расширятся до сокращения или увеличения штата тех или иных сотрудников, принадлежащих к этой группе.

Программное обеспечение:

- участвующее в обработке защищаемой информации;
- обеспечивающее безопасность хранения и передачи защищаемой информации.

Технические средства:

- зависимые от ПО (напр., компьютеры на рабочих местах, серверы);
- независимые от ПО (напр., энергоснабжения).

При таком делении ОМ напрямую могут взаимодействовать только с персоналом (Ч). Персонал в свою очередь может оказывать влияния как на ТС, так и на ПО. Также ТС и ПО могут взаимодействовать между собой, но ПО может влиять только на определенную группу ТС. Для наглядности отразим это на следующей схеме (рисунок 2).

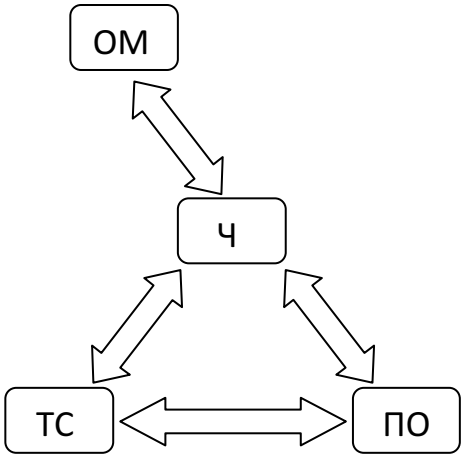

Рисунок 2. Схема взаимодействия элементов автоматизированной системы

Определив все виды взаимодействия элементов системы, можно составить развернутые матричные представления факторов аналогично с представлением представленным выше.

После выбора и описания всех возможных состояний элементов АС, негативно влияющих на защищенность информации, необходимо количественно оценить их влияние, выработать порядок генерации данных состояний, описать возможные меры по противодействию данным влияниям и их количественную оценку, выбрать методы оценки эффективности действий пользователя.

Для оценки количественного влияния факторов, негативно влияющих на защищенность информации, и мер противодействия можно прибегнуть к требованиям стандартов и экспертным оценкам [6]. Стоит отметить, что на данной стадии будут закладываться те

навыки и принципы, которые приобретет и которыми будет руководствоваться человек, прошедший обучение по данной методике, поэтому от грамотной настройки количественных показателей будет во многом зависеть эффективность обучения. Кроме того, не стоит забывать, что модель должна соответствовать реальному объекту, а на практике воздействие одного и того же негативного фактора может иметь различную критичность. Поэтому количественное влияние для негативных факторов не должно быть фиксированным (в то время как меры противодействия как раз наоборот должны иметь постоянное значение), а скорее носить случайный характер, но иметь некоторое среднее. Это усилит уровень детализации модели, но значительно усложнит оценку пользовательского решения. Также количественное влияние должно быть представлено в таком виде, в котором пользователь сможет визуально оценить угрозу как отдельного фактора, так и угрозу набора факторов, формирующих ситуацию.

Множество состояний, в которых может находиться объект защиты, описанное выбранной факторной моделью, генерируется путем комбинирования списка факторов и вариации их количественного влияния. Генерацию списка негативных факторов можно проводить случайным образом, но для большего соответствия модели реальному объекту стоит учесть, что факторы не являются равновероятными. Обучаемому необходимо будет каждый раз при использовании данного программного комплекса формировать комплекс мер в соответствии со своими теоретическими знаниями для максимально эффективного устранения предложенных угроз. Анализируя результат каждого решения, пользователь сможет делать выводы об эффективности его реакций на предложенную ситуацию.

Также немаловажную роль будет иметь и само описание факторов. Рассмотренное ранее представление факторов формализует их описание, что может негативно сказаться на эффективности обучения. Частично решить эту проблему можно путем составления списка элементов каждой подсистемы (напр., в программное обеспечение могут входить: ОС, брандмауэры, антивирусы, офисное ПО и т.д.). Для описания и расширения списка факторов стоит рассмотреть и существующие стандарты в области информационной безопасности (таких как ГОСТ Р ИСО/МЭК 15408-2002).

Отдельного внимания также заслуживает список мер по нейтрализации негативного воздействия на защищенность информации, в котором основным показателем эффективности принятых мер будет их стоимость. Но далеко не все меры имеют стоимость. Существует ряд мер, таких как инструктаж, почтовая рассылка и т.п., которые не будут иметь стоимости. Очевидно, что в таком случае они будут наиболее эффективными, и для каждой сгенерированной ситуации можно будет применять сначала все возможные меры с нулевой стоимостью, вне зависимости от самой ситуации и значений факторов. Чтобы

избежать подобных тривиальных решений, список мер для каждой задачи можно ограничить в зависимости от количества сгенерированных факторов и бесплатных мер, которые будут иметь эффект в данной ситуации. Такое ограничение не противоречит “поведению” реального объекта защиты, а скорее, наоборот, может быть интерпретировано тем, что данные меры требуют физических и временных затрат, что, опять же, позволяет улучшить соответствие автоматизированной системы и разработанной модели.

С учетом описанных выше свойств параметров модели необходимо, чтобы программная реализация имела возможность хранения больших объемов многомерных данных и их связей, а также возможность редактирования списка негативных факторов, мер противодействия и настройки их количественных показателей напрямую, без изменения программного кода. Реализовать эти требования можно, используя при разработке базы данных, представив все данные в виде трех таблиц:

1) список негативных факторов и диапазона значений их критичности;
2) список мер по нейтрализации негативного воздействия с указанием их количественного влияния;
3) вспомогательная таблица для хранения списка элементов автоматизированной системы.

Общую схему взаимодействия таблиц можно представить следующим образом (рис.3).

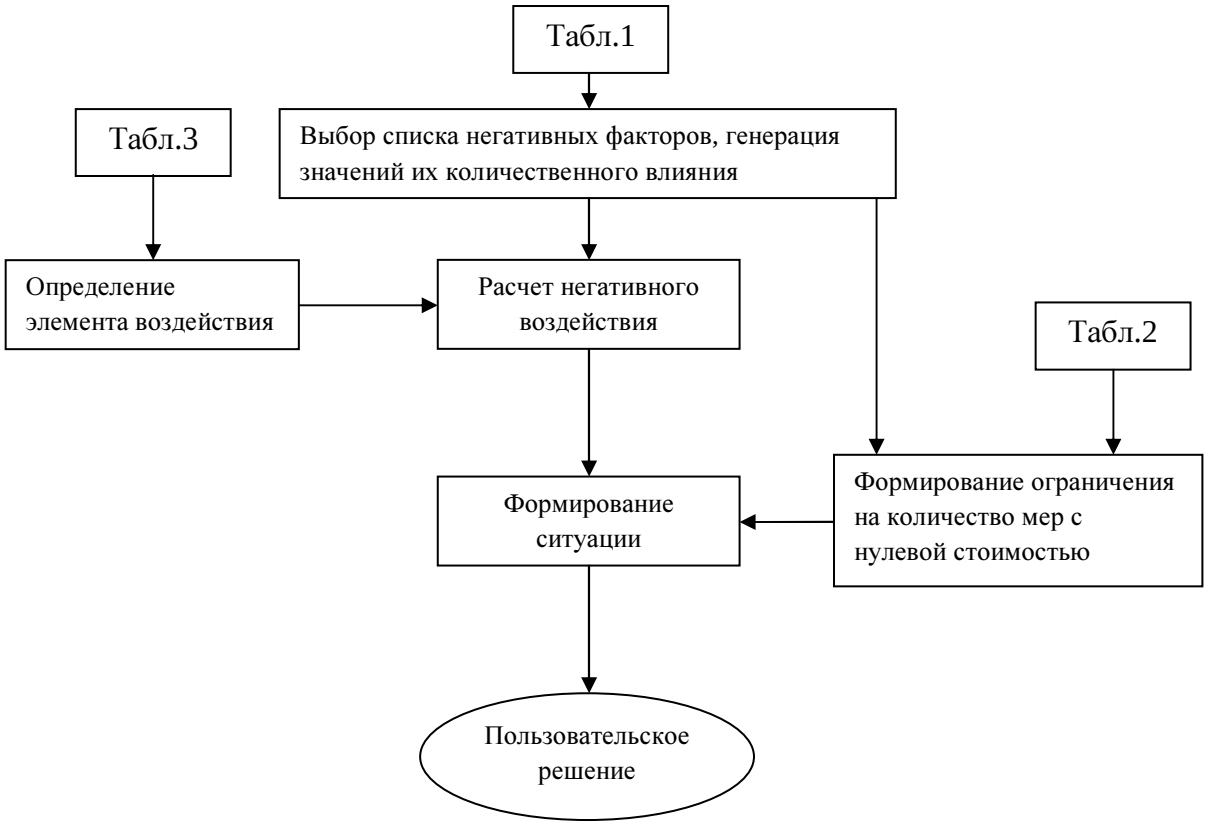

Рисунок 3. Схема взаимодействия таблиц

Так как целью данной работы является не точное моделирование процесса обеспечения информационной безопасности в конкретной АС, а обучение и проверка навыков специалиста по защите информации, при проектировании можно делать акцент на различные принципы защиты информации в АС (как наиболее общие, так и свойственные какому-либо классу АС, или вообще моделировать точно определенный объект защиты). Ситуации также можно задавать заранее или использовать случайный порядок генерации.

С учетом сформированных требований и выбранных методов было разработано программное обеспечение. Ниже приведен его интерфейс (рисунок 4).

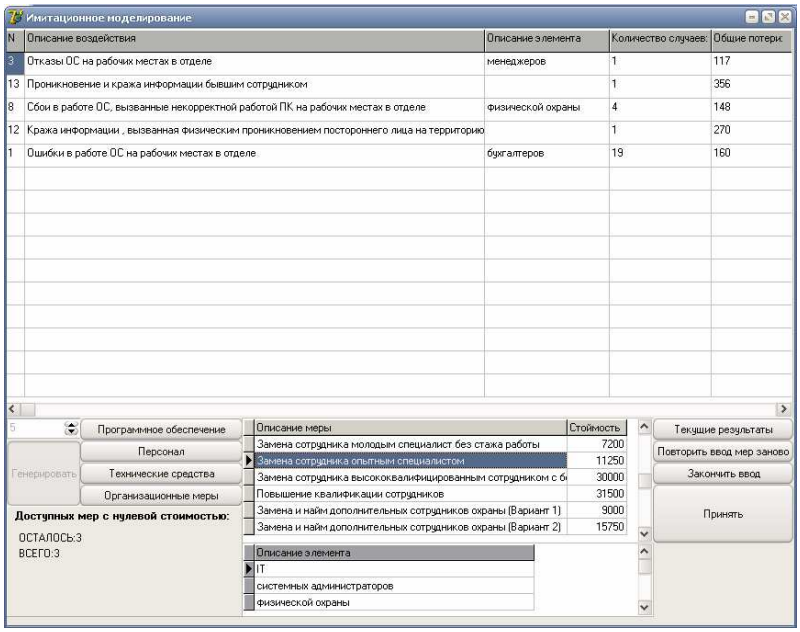

Рисунок 4. Интерфейс программного обеспечения

Немаловажным является и сам процесс обучения с помощью описываемой образовательной технологии. Логично построить задания так, чтобы уровень сложности переходил от простого к сложному. Все задания разделены на три лабораторных работы (табл.1).

Таблица 1. Список лабораторных работ

Название	Основная направленность	Состав
Лабораторная работа 1	Развитие и проверка навыков формирования комплекса мер, с помощью которого можно нейтрализовать некоторые наиболее распространенные угрозы безопасности информации.	Три ситуации, с заранее продуманными значениями и списком факторов.
Лабораторная работа 2	Формирование навыков нейтрализации негативного воздействия на независимые ситуации, связанные с угрозой безопасности информации.	Три набора ситуаций, с разным количеством факторов в каждом из наборов. Список факторов для каждой ситуации выбирается случайно.
Лабораторная	Развитие и проверка навыков	Одна ситуация с

работа 3	формирования комплекса мер по нейтрализации негативного воздействия на ситуации, связанные с угрозой безопасности информации и поддержания состояния защищенности информации в АС в условиях ограниченных ресурсов.	режимом пошагового выполнения и ограничением на используемые ресурсы.

Первые несколько заданий предполагают не только приобретение профессиональных навыков, но и ознакомление с программным продуктом. Сначала обучаемому предлагается несколько заранее подготовленных ситуаций, состоящих из небольшого количества наиболее распространенных случаев, связанных с угрозой безопасности информации. На этом этапе формируются простые комплексы мер, и вместе с тем происходит ознакомление с общим списком мер и их классификацией.

На следующем этапе факторы, негативно влияющие на безопасность информации, генерируются случайно, а их количественное влияние генерируется около некоторого среднего, определенного для каждого отдельного фактора в пределах заданного отклонения. Очевидно, что в данном случае сгенерированные ситуации будут отличаться друг от друга по сложности, поэтому на данном этапе предполагается, что обучаемому будет предоставлено несколько ситуаций, а результатом будет некоторое среднее из результата каждой. При этом важно не получить наибольший результат по одной из ситуаций, а выработать эффективный комплекс мер для каждой из них, вне зависимости от сложности задания. Такое усложнение заданий на этом этапе обусловлено тем, что навыки, приобретенные при выполнении первых заданий, дают представление о стандартных методах реакции на негативные воздействия на безопасность информации в АС, т.к. для ситуаций, состоящих из случайного набора факторов, типовые комплексы мер отсутствуют, для получения хорошего результата необходим более глубокий уровень понимания процессов, связанных с угрозой безопасности информации в АС, и мер противодействия.

Поскольку в рамках описываемой методики в качестве моделируемого объекта защиты рассматривается АС, то рассмотрение ее как набора отдельных независимых ситуаций не будет являться достаточно точной моделью, т.к. автоматизированная система не статична, а существует во времени, и обеспечение безопасности происходит непрерывно на всех этапах ее функционирования. Поэтому следующий комплекс заданий представляет собой ряд последовательных ситуаций, где решение одной влияет на все последующие. Для большего сходства модели с реальным объектом ресурсы для каждого задания ограничены.

Несмотря на то, что образовательная технология, представленная в данной статье, способна решать те задачи, для которых она разработана, она не лишена недостатков и имеет свои перспективы дальнейшего развития. В частности, существует проблема

автоматического определения эффективного комплекса мер для случайно сгенерированных ситуаций. Это связано с характером взаимосвязей между списком негативных воздействий и мер противодействия, а также наличием мер с нулевой стоимостью. Разработка алгоритма выработки таких решений является приоритетной задачей, т.к. это существенно повысит объективность оценки пользовательских решений. Кроме того, такой алгоритм будет крайне полезен при настройке взаимосвязей между негативными факторами и мерами противодействия. Также одним из направлений развития является разработка сетевой версии данной технологии. Это даст возможность удаленно выполнять задания, хранить базу данных только на серверной части программного комплекса, отдельно от клиентской части, а также разрабатывать версии программного обеспечения, в котором список угроз информационной безопасности будет формировать человек в режиме реального времени, что позволит проводить обучение в режиме соревнований. Не стоит забывать и про другие области профессиональной деятельности, в которых важным является навык принятия решений в условиях недостаточной информации. Выбранная архитектура программного комплекса позволяет путем замены базы данных и без особого вмешательства в программный код адаптировать данное программное обеспечение под обучение на различных специальностях.

Выводы

В заключение хотелось бы отметить, что разработанная образовательная технология способна совершенствовать множество профессиональных и общекультурных компетенций обучаемого, к числу которых относятся: принятие управленческих решений; разработка и исследование модели автоматизированных систем; проведение анализа защищенности автоматизированных систем; формирование комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированной системы; проведение анализа рисков информационной безопасности автоматизированной системы и др. Поэтому его можно применять в ходе учебного процесса, для повышения эффективности обучения. Причем, основная направленность программного комплекса заключается в тренировке навыка принятия управленческих решений в условиях неполной информации и риска. Технологии, основанные на факторном анализе, одна из которых представлена в статье, позволяют формировать навыки действий в определенной ситуации и ориентируют на выполнение реальных задач практической деятельности.

Список литературы

1. Бурдин О. А., Кононов А. А. Комплексная экспертная система управления информационной безопасностью Авангард // Информационное общество. М.: Изд-во ИРИО, 2002. Вып. 1. С. 38-44.
2. Домарев В. В. Модель и программа оценки систем защиты. URL: http://www.security.ukrnet.net/modules/news/article.php?storyid=48.
3. Золотарев В. В. О применении факторного анализа в задачах оценки защищенности элементов автоматизированных систем / В. В. Золотарев, Е. А. Данилова / Вестник СибГАУ им. акад. М. Ф. Решетнева 2010. Вып. 3 (29). С. 60-64.
4. Организационный подход к проектированию мультиагентной системы поддержки принятия решений по защите персональных данных / Васильев В. И., Белков Н. В. / Известия Южного федерального университета. Технические науки. 2011. Т. 125. № 12. С. 14-24.
5. Система Поддержки Принятия Решений по Защите Информации «ОАЗИС» / Бондарь И. В., Гуменникова А. В., Золотарёв В. В., Попов А. М. / Программные продукты и системы. 2011. № 3. С. 46.
6. Управление риском на основе качественных показателей / *Золотарев В. В.* Прикладная дискретная математика. Приложение. 2009. № 1. С. 105-107.
7. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность», утвержден приказом МинОбрНауки от 28.10.2009 №496.
8. Digital Security Office 2006**:** система анализа информационных рисков и оценки соответствия системы управления ИБ международным, национальным и корпоративным стандартам в области информационной безопасности. URL: http://www.dsec.ru/products/dsoffice/.
9. OCTAVE Method Implementation Guide, 2001 URL: http://www.cert.org/octave/octavemethod.html

Работа выполнена при поддержке Краевого фонда поддержки научной и научно-педагогической деятельности.

Рецензенты:

Петров М. Н., д.т.н., профессор, зав. кафедрой электронной техники и телекоммуникаций СибГАУ, г. Красноярск.

Шлепкин А. К., д.ф.-м.н., зав. кафедрой прикладной математики КрасГАУ, г. Красноярск.