УДК 378.016:004.056.5

Миронова А. А., Шабуров А. С.

МОДЕЛЬ РАЗРАБОТКИ УЧЕБНО-ЛАБОРАТОРНОГО КОМПЛЕКСА ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В данной статье рассматриваются требования по подготовке кадров в области обеспечения информационной безопасности, которым должен соответствовать специалист по защите информации. Анализируются проблемы учебного процесса, обусловленные разнообразными причинами. Предлагается теоретико-множественная модель разработки учебно-лабораторного комплекса, позволяющего сформировать заданный набор учебных моделей для подготовки специалистов по защите информации

Ключевые слова: *учебно-лабораторный комплекс, средство защиты информации, теоретико-множественная модель, технология виртуализации*

Mironova A. A., Shaburov A. S.

MODEL FOR DEVELOPMENT EDUCATIONAL LABORATORY COMPLEX TO TRAIN SPECIALISTS IN INFORMATION PROTECTION

The article discusses the requirements for training in the field of information security, which must comply with information security specialists. The problems of the educational process due to various causes. It is proposed to set-theoretic model of the development of teaching and laboratory complex, which allows to generate a given set of training modules for the training of information security specialists

Keywords: *teaching and laboratory facilities, protection of data, set-theoretic model, virtualization technology*

Обеспечение безопасности национальных интересов невозможно без рассмотрения и решения первостепенных проблем, к которым, безусловно, относится необходимость подготовки компетентных специалистов по защите информации. Заказчиками подобных специалистов являются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, государственные учреждения, организации и предприятия оборонной промышленности, органы местного самоуправления, а также учреждения, организации и предприятия негосударственной формы собственности.

Требования по подготовке специалистов по защите информации определены на уровне государственных стандартов, содержащих следующие основные пожелания к знаниям, профессиональным навыкам и компетенциям выпускников:

• экспертный уровень владения персональным компьютером;

• владение иностранным языком на уровне чтения технической документации;

• знание нормативно-правовой базы, государственных стандартов, руководящих документов в сфере информационной безопасности;

• знание порядка защиты информационных систем от несанкционированного доступа, умения настройки и конфигурации современных решений в области защиты информации (средств защиты от НСД, межсетевых экранов, систем обнаружения вторжений и т. п.);

• знания современных стандартов шифрования и опыт работы с техническими и программными средствами шифрования;

• опыт разработки регламентов и политик безопасности, а также опыт проведения аудита информационной безопасности [1].

Из вышеперечисленных требований следует вывод, что выпускник вуза должен обладать универсальными знаниями в достаточно разнообразных областях, что обуславливает ряд проблем качества подготовки кадров, соответствующих быстро меняющимся современным условиям.

Из-за универсальности направления подготовки в данной области уместить необходимые для изучения и освоения знания и умения в нужных объемах в стандартную программу обучения становится сложно. Следовательно, первой проблемой подготовки кадров становится поверхностное изучение аспектов специальностей, приводящее к несоответствию характеристик выпускника вуза реальным условиям работы специалиста по защите информации.

Вторая проблема обучения - это недостаточная укомплектованность лабораторных баз современными учебно-лабораторными стендами, средствами защиты информации, методическими материалами. Отсюда вытекает и третья проблема – недостаточность практической подготовки студентов.

Четвертой проблемой становится нехватка преподавателей, которые бы являлись опытными сотрудниками подразделения безопасности в организации, где информационная безопасность является одним из важнейших аспектов ее функционирования.

Кроме того, в вузах обычно недостаточно внимания уделяется социально-психологическим аспектам подготовки – это пятая проблема подготовки специалистов в области безопасности информации [2].

В данных условиях развитие лабораторной базы для специалистов по защите информации, а также оперативная адаптация лабораторных и практических занятий для изучения наиболее актуальных вопросов информационной безопасности является одной из задач совершенствования системы подготовки кадров.

Создание новых учебно-лабораторных комплексов для исследования защищенности информационных систем позволит сформировать необходимые практические навыки и выработать требуемые компетенции для будущей профессиональной деятельности студентов. Особенно важной составляющей подготовки специалистов по защите информации является их готовность к защите от кибератак на информационно-управляющие системы критически важных объектов [3].

Интенсивное развитие технологий и появление на рынке безопасности значительного выбора разнообразных средств защиты, заставляют решать задачу оперативной корректировки учебных задач в соответствии актуальным потребностям. Кроме того, необходимость быстрого переориентирования программы подготовки для конкретных условий региона, отрасли, ведомства, предприятия, дороговизна современных средств защиты информации заставляют переводить процесс обучения на уровень модельных представлений систем защиты информации.

Предлагаемая теоретико-множественная модель (ТММ) позволяет подобрать оптимальный состав моделей учебно-лабораторного комплекса (УЛК), в свою очередь, позволяющего сформировать необходимый набор компетенций выпускника [4].

В интересах фундаментальной подготовки специалистов центральной задачей изучения методов и средств защиты информации является приобретение компетенций по их рациональному применению в зависимости от типа информационной системы, характера угроз безопасности информации, и т.п.

Основной целью, которая ставится при разработке ТММ, является возможность понимания и освоения обучаемыми этих компетенций методом лабораторного исследования. Процесс лабораторного исследования позволяет с наибольшей наглядностью и высоким коэффициентом усвоения приобретать необходимые знания и навыки, а также позволяет существенно сократить время необходимое для подготовки специалиста для конкретных условий эксплуатации системы защиты информации.

Значительное разнообразие способов и средств защиты информации предполагает объективное существование множества адекватных моделей Ω, элементы которого могли бы служить объектами лабораторных исследований. Понятие адекватности моделей следует рассматривать в двух аспектах: адекватность прототипу (корректность описания соответствующей информационной системы) и адекватность главной цели обучения – приобретение необходимых компетенций.

Согласно специализации учебного заведения как места проведения планируемых лабораторных занятий на первом этапе построения необходимого класса моделей можно ограничиться рассмотрением подмножества $\Omega^{/} \subset \Omega$ исходного набора моделей Ω, что оправдывается содержанием государственного заказа в части касающейся квалификационных характеристик выпускника и по своему математическому смыслу может быть описано оператором гомоморфизма (сжатия):

$$\Gamma : \Omega \to \Omega^{/} \qquad (1)$$

Искомое подмножество учебных моделей Ω_y, с одной стороны, должно принадлежать агрегированному подмножеству $\Omega^{/}$, то есть $\Omega_y \subset \Omega^{/}$.

С другой стороны, каждому элементу ω множества Ω_y следует предъявить обязательные требования:

1) полный охват изучаемых способов и средств защиты информации;

2) ограниченное машинное время моделирования, поглощающее резерв учебного времени T_y.

Первое требование приводит к необходимости рассмотрения отображения:

$$\alpha : \Omega^{/} \to \Pi_{\pi}, \qquad (2)$$

где π – множество средств защиты информации, $\Pi(\pi) = \Pi\pi$ – булеан (множество всевозможных наборов методов и средств защиты).

Тогда в идеальном случае, предполагающем возможность в рамках каждой учебной модели $\omega \subset \Omega_y$ обучения всем способам и средствам ЗИ, данное требование примет вид предиката:

$$(\forall \omega \in \Omega^{/}) P(\alpha(\omega) = \pi \to \omega \in \Omega_y) \qquad (3)$$

Если мощность полученного по правилу (3) множества Ω_y не соответствует общему числу обучаемых K

$$N = |\Omega_y| < K \qquad (4)$$

где N – число учебных вариантов лабораторных исследований, то на множестве Ω_y придется находить наборы моделей $\rho^{\Omega_y} \in \Pi_{\Omega_y}$ позволяющие достигнуть цель обучения, т. е. заданных компетенций:

$$(\forall \rho^{\Omega_y} \in \Omega^{/}) P(\bigcup^{\rho^{\Omega_y}} \alpha(\omega) = \pi \to \rho^{\Omega_y} \in \Omega_y) \qquad (5)$$

В данном случае на большем числе учебных вариантов исследования, поскольку

$$|\Pi_{\Omega_y}| = |\Omega_y|^2 >> |\Omega_y| \qquad (6)$$

откуда следует

$$|\Pi^{/}_{\Omega_y}| > |\Omega_y| \qquad (7)$$

где $\Pi^{/}_{\Omega_y}$ есть подмножество булеана Π_{Ω_y}, элементы которого удовлетворяют предикату (3), либо предикату (5). Данные рассуждения поясняются с теоретико – множественных позиций на рис 1.

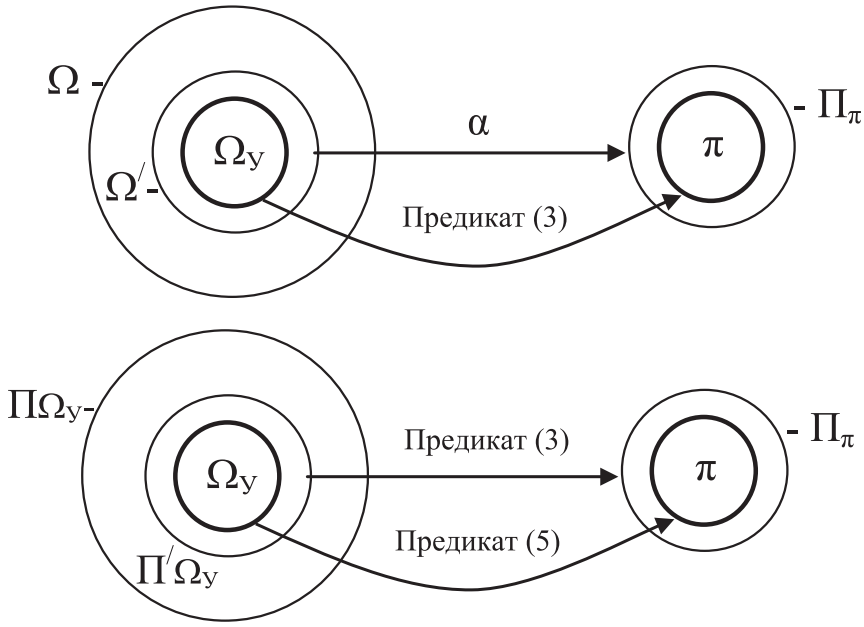

Рис. 1. Теоретико-множественная интерпретация процедуры образования множества учебных моделей УЛК

Множество учебных моделей Ω_y, предназначенных для лабораторных исследований, может быть описано прямым перечислением своих элементов в виде базы данных, что не всегда приемлемо из-за значительных потребностей памяти при большой его мощности. Кроме того, данное множество может быть задано характеристическим признаком решаемой задачи, что позволит создавать модели непосредственно перед лабораторными исследованиями. В любом случае целесообразно создать программный инструмент оперативного перечисления учебных моделей.

Применение подобного приема генерирования необходимого набора учебных моделей позволит ориентировать обучение на возможности рационального применения современных технологий обработки информации и ее защиты, например при использовании технологии виртуализации.

Например, в случае обеспечения антивирусной защиты виртуальных серверов, или рабочих станций использование классических антивирусных продуктов, предполагающих установку на каждый защищаемый узел, является нецелесообразным. Более рациональным будет использование антивирусного решения, устанавливаемого на гипервизор и выполняющего сканирования всех виртуальных серверов и рабочих станций, запущенных на физическом узле.

Применительно к обеспечению защиты от сетевых атак также более рациональным является использование решения, устанавливаемого на гипервизор. Такое решение позволит снизить использование аппаратных ресурсов физического узла, а также эффективно противостоять различным методикам сокрытия сетевого трафика5. Подобные решения могут стать основаниями для построения учебных моделей УЛК и их дальнейшего исследования.

Таким образом, необходимость освоения заданных компетенций специалистами по защите информации требует развития учебно-лабораторной базы для их подготовки, совершенствования методических приемов приобретения знаний, умений и практических навыков. Исследования в области совершенствовании технологии обучения, направленные на оптимизацию и совершенствование образовательного процесса помогут адаптировать подготовку выпускников к современным требованиям.

Примечания

1. Редакция журнала «Information Security» Специалист информационной безопасности // Журнал «Information Security/Информационная безопасность» № 4, 2013, с. 12.

2. Павлов А. Комплексные учебные программы для специалистов информационной безопасности // Журнал «Information Security / Информационная безопасность» № 3, 2014, с. 14-15.

3. Южаков А.А., Шабуров А.С., Рашевский Р.Б. О разработке учебно-лабораторного комплекса для исследования защищенности критически важных объектов // Вестник УрФО. Безопасность в информационной сфере.- Челябинск. Изд. центр ЮУрГУ, 2012. — № 3-4(5-6). — С.54 – 59.

4. Екимов О.Б. Методика разработки учебно-лабораторного комплекса для исследования систем защиты информации сложных военно-технических объектов: диссертация на соискание ученой степени кандидата технических наук. – Пермь: Пермский военный институт ракетных войск, 2003. – 125с.

5. Шабуров А.С., Рашевский Р.Б. О практическом применении технологии VMWare vShield App для обеспечения безопасности информационных систем персональных данных // Вестник УрФО. Безопасность в информационной сфере.- Челябинск. Изд. центр ЮУрГУ, 2014. — № 4(14). — С.27 – 32.

Миронова Анна Алексеевна, студент, Пермский национальный исследовательский политехнический университет. E-mail: mir550@yandex.ru

Шабуров Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики ПНИПУ, сотрудник РУНЦ по информационной безопасности, г. Пермь. E-mail: shans@at.pstu.ru

Anna Mironova, a student, Perm National Research Polytechnic University, Perm. E-mail: mir550@yandex.ru

Shaburov Andrew, Associate Professor, Candidate of Technical Sciences, National Research Polytechnic University, Perm. E-mail:shans@at.pstu.ru