ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Разработка комплекта учебных материалов и заданий для самостоятельной работы слушателей курсов повышения квалификации «Методы и средства защиты компьютерной информации»

Методические указания по использованию комплекта

Автор: доцент кафедры
алгебры и дискретной математики
Н.И. Синадский

Екатеринбург
2008

Методические указания по использованию комплекта учебных материалов и заданий для самостоятельной работы слушателей курсов повышения квалификации «Методы и средства защиты компьютерной информации»

Предлагаемый комплект учебных материалов и заданий предназначен для самостоятельной работы слушателей курсов повышения квалификации «Методы и средства защиты компьютерной информации» при Региональном учебно-научном центре «Информационная безопасность» при ГОУ ВПО Уральский государственный университет им. А.М. Горького.

Кроме того, комплект может быть полезен для специалистов, отвечающих за безопасность информационных объектов, для преподавателей и студентов ВУЗов, изучающих вопросы безопасности современных информационных технологий.

Цель комплекта — предоставить слушателям курсов возможность изучить методы и средства защиты компьютерной информации на примере имеющихся на российском рынке специализированных программно-аппаратных систем. Основной акцент при изучении делается на практическое изучение материала.

В рамках лекционного курса слушателям дается информация по основам защиты информации, методам и средствам. Весь лекционный материал представлен в виде презентаций в формате Microsoft PoverPoint. В целях интенсификации процесса обучения не предполагается фиксация слушателями в учебных тетрадях всех текстовых и схематичных материалов, представленных в презентациях. Для подготовки к зачетным мероприятиям, а также для последующего использования в практической деятельности все лекционные материалы представлены в данном комплекте. Лекционные материалы содержатся в каталоге комплекта «Презентации».

При изучении раздела курса «Нормативные и организационно-правовые основы обеспечения информационной безопасности» наряду с соответствующим лекционным материалам слушатели должны самостоятельно ознакомиться с основными нормативными документами в области информационной безопасности. В каталоге комплекта «Нормативные документы» содержится перечень актуальных и выведенных из употребления нормативно-правовых актов, и сами документы, разложенные по подкаталогам в зависимости от их статуса и назначения. Указанные документы, конечно, не являются исчерпывающим набором, однако представляют тот необходимый минимум, на который даются ссылки в лекционном курсе. Вместе с тем, в практической деятельности при применении указанных документов необходимо выполнять постоянное обновление имеющегося перечня. Также следует указать на возможное наличие опечаток и иных неточностей в текстах представленных на диске документов. Таким образом, представленный в каталоге материал предполагается использовать только для образовательных целей.

Практические задания для выполнения представлены в текстах четырех учебных пособий и лабораторного практикума:

1. АНАЛИЗ И ВОССТАНОВЛЕНИЕ ДАННЫХ НА НОСИТЕЛЯХ С ФАЙЛОВОЙ СИСТЕМОЙ NTFS: учебное пособие / Н. И. Синадский; научный редактор канд. техн. наук, доц. В.В. Бакланов. Екатеринбург: ГОУ ВПО УГТУ–УПИ, 2007. –136 с.
2. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. ПРАКТИЧЕСКИЙ КУРС: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург: УГТУ-УПИ, 2008. – 248 с.
3. ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: учебное пособие / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков; науч. ред. д-р техн. наук, проф. Н. А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008. – 182 с.
4. УГРОЗЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: учебное пособие / Н.И. Синадский, О.Н. Соболев. Екатеринбург: Изд-во Урал. ун-та, 2000. – 85 с.
5. АДМИНИСТРИРОВАНИЕ И БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ НА БАЗЕ ОПЕРАЦИОННЫХ СИСТЕМ MS WINDOWS 2000, XP. Лабораторный практикум. / Н.И. Синадский. Екатеринбург: УрГУ, 2004. — 52 с.

Указанные пособия в формате Adobe PDF представлены в каталоге комплекта «Учебные пособия».

По мере изложения теоретического материала в пособиях читателям предлагаются практические задания, обозначенные абзацем ***«ВЫПОЛНИТЬ!»***. Выполнение заданий, а также ответы на содержащиеся в них вопросы являются необходимым условием освоения учебного материала.

Для отработки практических заданий применяются подготовленные виртуальные образы операционных систем Microsoft Windows 2000 и Windows XP с уже установленными средствами защиты. Образы содержатся в каталоге комплекта «VMWare-образы курс СЗИ». Для работы с образами в корневом каталоге комплекта содержится дистрибутив свободно распространяемого программного комплекса VMWare Player (файл VMware-player-2.0.0-45731.exe).

Кроме того, для выполнения заданий по соответствующим темам требуется дополнительное программное обеспечение. Для отработки заданий предлагается использовать свободно распространяемое программное обеспечение либо демонстрационные версии коммерческих программ. Представленные в соответствующих подкаталогах каталога комплекта «Занятия» дистрибутивы таких программ предлагается устанавливать также в образы виртуальных систем.

Работа с образами виртуальных систем решает ряд методических проблем при выполнении заданий. В частности, решается проблема

необходимости присутствия разных систем на одном рабочем месте. Изучение принципов работы СЗИ при проведении практических занятий требует развертывания каждой из систем на отдельном компьютере. Установленные механизмы защиты полностью блокируют возможность проведения на данном компьютере занятий по изучению других тем и использованию его в повседневной деятельности. Для проведения занятий средствами VMware Workstation заранее создается образ операционной системы MS Windows 2000 или XP, который может быть сохранен и размножен для дальнейшей установки различных СЗИ. Каждое СЗИ устанавливается и сохраняется в отдельном файле-образе. Размер файла-образа — до 2 Гб, что позволяет на одном рабочем месте иметь более десятка различных систем в разных конфигурациях. После сжатия файла-образа программой-архиватором его объем уменьшается до 500-600 Мб, что позволяет сохранять и переносить образы систем на обычных CD-ROM дисках.

Второй решаемой проблемой является необходимость использования в компьютерных классах и на компьютерах слушателей, используемых ими для самостоятельной работы, разнотипных аппаратных сред. Особенностью виртуальных машин VMware Workstation является возможность работы образа на любом компьютере, удовлетворяющем определенным требованиям по объему свободного дискового пространства и оперативной памяти (от 128 Мб ОЗУ). Таким образом, полученный образ системы с установленным СЗИ может быть легко размножен практически в любом компьютерном классе или, например, на домашнем компьютере слушателя.

Третьей решаемой проблемой является то, что для изучения одного средства защиты требуется до 6 часов занятий, в то время как чаще всего в расписании учебных групп отведено 4, а то и 2 часа в неделю. Следовательно, лабораторная работа должна быть прервана на определенном этапе с возможностью ее продолжения на очередном занятии. Система VMware Workstation предоставляет возможность «усыпить» (команда ***Power ⇒ Suspend***) операционную систему в определенном состоянии и «разбудить» ее, возобновив изучение с этого же момента. Таким образом, слушателям при возобновлении занятий не приходится повторно выполнять настройки ОС и средств защиты и, следовательно, нет необходимости искусственно прерывать ход лабораторной работы.

Четвертой проблемой, легко решаемой с применением системы VMware Workstation, является необходимость деления группы слушателей на подгруппы и проведения занятий в разное время на одних и тех же рабочих местах, что требует для каждой подгруппы имитации собственного отдельного компьютера. Проблема решается простым дополнительным копированием исходного образа ОС с СЗИ для очередной подгруппы.

Кроме того, система VMware Workstation позволяет в реальном режиме времени с использованием дискового редактора исследовать изменения, происходящие на жестком диске в ходе активизации защитных механизмов.

Также система виртуальных машин позволяет организовать на одном компьютере небольшую до 3-4 узлов компьютерную сеть и отработать вопросы защиты сетевых соединений.

Для анализа сетевых соединений и сетевых атак достаточно двух узлов. Один в этом случае играет роль атакующего, на нем также может вестись захват сетевого трафика, а другой — роль атакуемого. В качестве атакующего целесообразно использовать основную операционную систему, в качестве атакуемого — виртуальный компьютер. Для работы с межсетевыми экранами может понадобиться дополнительно третий виртуальный компьютер, выполняющий роль, например, фильтрующего маршрутизатора. Для организации VPN-сети необходимо большее число сетевых узлов, в этом случае целесообразно использовать два основных компьютера с работающими на них виртуальными системами.

При наличии образов операционных систем настройка сетевых соединений в системе VMware Workstation производится следующим образом. Прежде всего определяется IP-адрес основного компьютера и его маска подсети, например, при помощи команды ipconfig.

Далее необходимо вызвать настройки каждой из используемых виртуальных машин (команда в главном меню VMware Workstation ***Edit*** $\Rightarrow$ ***Virtual Mashine Settings…***) и в разделе Hardware выбрать настройки виртуального сетевого адаптера. Установить пункт «Bridget. Connected directly to the physical network» (Прямое соединение к физической линии).

Далее IP-адрес виртуального компьютера настраивается обычным образом с учетом IP-адреса и маски подсети основного компьютера. Теперь в сети присутствуют два независимых сетевых узла.

Сетевое взаимодействие узлов, в случае соответствия их маски подсети, легко проверить, например, командой Ping.