Я.Е. ПРОКУШЕВ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение надежной защиты информации при ее обработке, хранении и передаче с использованием средств вычислительной техники от несанкционированного доступа (НСД) со стороны нарушителей и воздействия вредоносного кода является важнейшим направлением деятельности специалистов в сфере информационной безопасности.

Эта точка зрения нашла свое подтверждение в содержании ФГОС направления подготовки бакалавриата 10.03.01 «Информационная безопасность» в виде обязательного изучения дисциплины «Программно-аппаратные средства защиты информации». В процессе преподавания этого предмета, наряду с обязательным рассмотрением теоретических вопросов, значительное внимание уделяется приобретению практических навыков использования различных средств программно-аппаратной защиты информации.

В книге, предлагаемой вниманию читателя, подробно описываются практические аспекты использования сертифицированных ФСТЭК РФ средств защиты информации Dallas Lock 8 и антивируса Kaspersky Endpoint Security 10 для Windows. Практикум состоит из лабораторных работ, выполнять которые рекомендуется в том порядке, в каком они приведены.

Работа со средством защиты информации от несанкционированного доступа (СЗИ от НСД) Dallas Lock 8. Рассматриваются вопросы настройки механизмов авторизации, контроля и аудита доступа пользователей к объектам файловой системы и внешним устройствам. Исследуются особенности настройки механизмов гарантированной очистки информации и замкнутой программной среды, использования криптографических методов защиты информации, настройки контроля целостности объектов.

Проблематика обеспечения защиты информации от воздействия вредоносных программ и сетевых атак рассмотрена с использованием средства антивирусной защиты информации Kaspersky Endpoint Security 10 для Windows.

Заключительная лабораторная работа посвящена изучению положений Постановления Правительства РФ от 01.11.2012 № 1119, Приказов ФСТЭК РФ № 21 от 18.02.2013 и № 17 от 11.02.2013.

Элементы графического интерфейса защитных программ могут иметь незначительные отличия от представленных в книге рисунков.

В практикуме раскрываются компетенции ФГОС направления подготовки бакалавриата 10.03.01 «Информационная безопасность»:

– ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

– ПК-3 – способностью администрировать подсистемы информационной безопасности объекта защиты;

– ПК-6 – способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

– ПК-9 – способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Также практикум может быть использован при подготовке студентов по ФГОС специальностей высшего образования:

– 10.05.02 и 10.05.03 при изучении дисциплины «Программно-аппарат-ные средства обеспечения информационной безопасности»;

– 10.05.05 при изучении дисциплины «Программно-аппаратные средства защиты информации».

Лабораторный практикум может использоваться как в процессе проведения аудиторных занятий, так и при осуществлении самостоятельной работы. Использование материалов учебного пособия возможно и в процессе преподавания дисциплины «Информационная безопасность» для студентов, обучающихся по ФГОС УГСНП 09.00.00 «Информатика и вычислительная техника».

Изложенный в книге материал способствует выполнению обобщенных трудовых функций профессиональных стандартов:

1) «специалист по защите информации в автоматизированных системах» – функция «обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации»;

2) «специалист по безопасности компьютерных систем и сетей» – функции «администрирование средств защиты информации в компьютерных системах и сетях».

Для выполнения заданий предпочтительнее использовать следующее программное и аппаратное обеспечение:

1) VMware Player или Virtual Box для запуска виртуальных машин, работающих под управлением операционных систем семейств Windows;

2) желательно наличие принтера, при его отсутствии можно использовать виртуальные принтеры;

3) учебная или коммерческая версии СЗИ от НСД Dallas Lock 8 редакций «К» или «С»;

4) средство антивирусной защиты Kaspersky Endpoint Security 10 для Windows с постоянной или временной (trial) лицензией;

5) пакет офисных программ MS Office или Open Office; 5) свободно распространяемый сетевой сканер Nmap;

6) средство просмотра pdf файлов Adobe Acrobat Reader или другое. Для выполнения лабораторных работ следует развернуть локальную сеть из виртуальных машин в соответствии с одной из схем, приведенных в приложении 1.

Свои пожелания или критические замечания относительно приведенного в книге материала можно высылать на электронный ящик автора:

yaroslav-prokushev@mail.ru