ПРОКУШЕВ Я.Е.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Практикум
для студентов, обучающихся
по специальностям и направлениям подготовки
09.00.00 «Информатика и вычислительная техника»,
10.00.00 «Информационная безопасность»,
направлению подготовки 38.03.05 «Бизнес-информатика»,
специальности 38.05.01 «Экономическая безопасность»

Санкт-Петербург
ИЦ «Интермедия»
2018

УДК 004.56(075.8)
ББК 32.81я73
П80

Автор:
Прокушев Ярослав Евгеньевич, канд. экон. наук, доцент, заведующий кафедрой организации и технологии защиты информации Белгородского университета кооперации, экономики и права

Главный редактор: Т.С. Кулакова
Техническая подготовка: В.Ю. Антипова
Дизайн обложки: А. Н. Федулова

П80 Прокушев Я.Е.
Информационная безопасность: практикум/ Прокушев Я.Е. – СПб.: ИЦ «Интермедия», 2018. – 288 с.: ил.

В практикуме рассмотрено применение встроенных защитных механизмов ОС Windows: управления доступом к каталогам и принтерам, аудита работы пользователей, настройки политик безопасности и технологии шифрования данных BitLocker. Рассмотрены особенности работы с сертифицированными ФСТЭК РФ межсетевыми экранами, средством антивирусной и криптографической защиты информации, аппаратным модулем доверенной загрузки, а также свободно распространяемым средством криптографической защиты информации TrueCrypt.

Книга предназначена для студентов, обучающихся по специальности «Экономическая безопасность», направлениям подготовки «Бизнес-информатика», «Информатика и вычислительная техника», «Информационные системы и технологии», «Прикладная информатика», «Программная инженерия», специальностям и направлениям подготовки, относящимся к УГСНП «Информационная безопасность». Материалы книги могут быть полезны практическим работникам в области информационной безопасности.

ISBN xxx-x-xxxx-xxxx-x

Учебное издание

Прокушев Ярослав Евгеньевич

Информационная безопасность

Подписано в печать 11.09.2017. Формат 60×88 1/16. Печать цифровая.
Усл. печ. л. 16,74. Тираж 500 экз. Заказ №
ООО «Издательский центр “Интермедия”». Адрес: 198334, Санкт-Петербург, ул. Партизана Германа, 41-218. Отпечатано с готового оригинал-макета в ООО «Арт-экспресс». Адрес: 199155, СПб., В.О., ул. Уральская, д. 17.

ISBN xxx-x-xxxx-xxxx-x	© ООО «Издательский Центр “Интермедия”», 2018 © Прокушев Я.Е., 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время умение обеспечить защиту информации при ее обработке с использованием средств вычислительной техники от несанкционированного доступа (НСД) к ней является одним из необходимых навыков, которым должны обладать специалисты не только в области информационных технологий, но и в экономической безопасности.

Для получения необходимых знаний, умений и навыков в учебном плане специальности «Экономическая безопасность», а также направлений подготовки «Бизнес-информатика», «Информатика и вычислительная техника», «Информационные системы и технологии», «Прикладная информатика», «Программная инженерия» предусмотрено изучение дисциплины «Информационная безопасность». В процессе преподавания этого предмета, наряду с рассмотрением теоретических вопросов, значительное внимание должно уделяться приобретению практических навыков настройки средств защиты информации. В практикуме, предлагаемом вниманию читателя, подробно описываются практические аспекты использования:

1) защитных механизмов, встроенных в операционные системы семейства Windows. В рамках их изучения рассматриваются:

– настройки политик безопасности в ОС Windows 7\8\10;

– особенности системы дискреционного управления доступом к объектам файловой системы и аудита работы пользователей;

– работа с системой шифрования *BitLocker*;

– возможности ОС Windows, позволяющие организовать замкнутую программную среду, ограничить использование внешних устройств и т.п.;

2) сертифицированных ФСТЭК РФ и свободно распространяемых средств криптографической защиты информации. Рассмотрены вопросы организации защищенной обработки файлов с использованием СКЗИ *VipNet SafeDisk 4.1* и популярного свободно распространяемого СКЗИ *TrueCrypt*;

3) сертифицированных ФСТЭК и ФСБ РФ межсетевых экранов, таких, как *VipNet Personal Firewall* и *TrustAccess*. Рассмотре-

на проблема организации защищенного сегмента в локальной вычислительной сети;

4) средства антивирусной защиты информации (САВЗ) *Dr. Web Security Space*.

При рассмотрении различных средств защиты информации уделено внимание методам организации защищенного многопользовательского режима обработки данных и противодействию распространенным угрозам информационной безопасности, таким, как неконтролируемое применение съемных USB-устройств, печать документов и использование ресурсов глобальной сети.

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

Также практикум может быть использован для организации учебного процесса студентов по направлениям подготовки и специальностям, относящимся к УГСНП 10.00.00 «Информационная безопасность» при изучении дисциплин, рассматривающих вопросы обеспечения информационной безопасности автоматизированных систем, применения криптографических и программно-аппаратных средств защиты информации.

Для выполнения заданий предпочтительнее использовать следующее программное и аппаратное обеспечение:

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

2) демонстрационные или коммерческие версии СКЗИ *VipNet SafeDisk*, МЭ *VipNet Personal Firewall*, МЭ *TrustAccess*, САВЗ *Dr. Web Security Space*;

3) желательно использование принтера, при его отсутствии можно применить виртуальные устройства печати;

4) пакет офисных программ *MS Office* или *Open Office*;

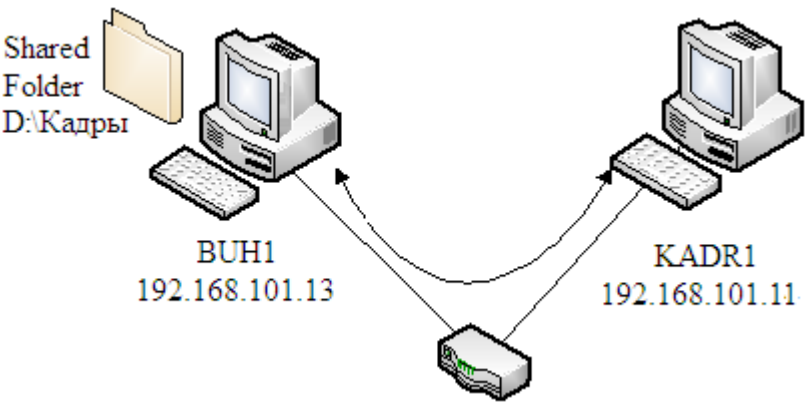
5) свободно распространяемый сетевой сканер *Nmap*.

Для выполнения лабораторных работ следует развернуть локальную сеть из виртуальных машин в соответствии со схемой, приведенной в приложении 1.

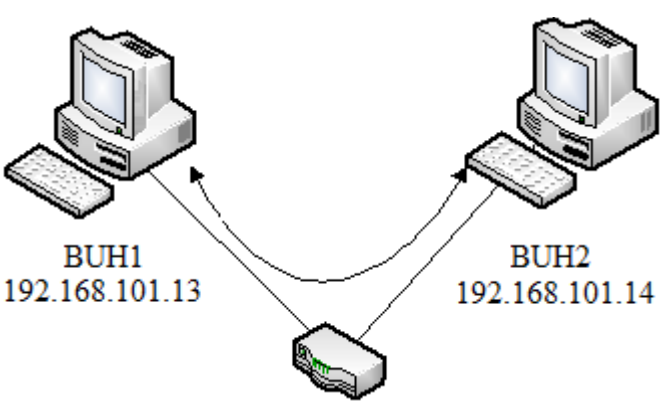
Критические замечания или пожелания относительно содержания приведенного в книге материала можно высылать на электронный ящик автора: yaroslav-prokushev2@mail.ru.

Приложение 1

Возможные схемы виртуальной сети
для выполнения лабораторных заданий



Стенд для выполнения лабораторных работ 1–8



Стенд для выполнения лабораторных работ 9–11