

УДК 34.028 (075.8)
ББК 67.404.3 я 73
К 63

Печатается по решению
редакционно-издательского совета
Северо-Кавказского федерального
университета

Рецензенты:

кандидат технических наук, профессор ***А. Ф. Чипига***,
доктор технических наук, профессор ***И. А. Калмыков***

К 63 Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / авт.-сост.: Лапина М. А., Марков Д. М., Гиш Т. А., Песков М. В., Меденец В. В. – Ставрополь: Изд-во СКФУ, 2016. – 242 с.

Пособие представляет лабораторный практикум, в котором рассматриваются вопросы содержания и последовательности работ по защите информации, построение модели угроз ИСПДн; составления модели угроз и модели нарушителя, изучение действующей нормативной документации объекта информатизации, исследования методов выбора рационального варианта системы защиты информации на основе экспертной информации.

Предназначено для преподавателей и студентов вузов, обучающихся по специальностям «Комплексное обеспечение информационной безопасности автоматизированных систем», «Организация и технология защиты информации», «Информационная безопасность автоматизированных систем».

УДК 34.028 (075.8)
ББК 67.404.3 я 73

© ФГАОУ ВПО «Северо-Кавказский
федеральный университет», 2016

ПРЕДИСЛОВИЕ

Учебное пособие (лабораторный практикум) предназначено для теоретической и практической подготовки специалиста к организации и проведению мероприятий по комплексному обеспечению информационной безопасности автоматизированных систем и выполнению лабораторных работ по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем».

Выполнение лабораторных работ студентами играет важную роль в формировании определенных образовательной программой **компетенций**:

ПК-12 – способностью проводить анализ защищенности автоматизированных систем;

ПК-13 – способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

ПК-20 – способностью разрабатывать политики информационной безопасности автоматизированных систем;

ПК-29 – способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;

ПК-33 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации.

Основные **задачи** дисциплины предусматривают предоставление знаний по вопросам комплексной защиты информации, об основных проблемах защиты информации таких как:

- порядок проведения инвентаризации и категорирования информационных ресурсов;

- порядок аттестации объектов информатизации на соответствие требованиям безопасности информации;

- порядок выявления угроз несанкционированного доступа к информации и специальных воздействий на нее в информационных и телекоммуникационных системах;

- изучение способов и средств защиты персональных данных.

Выполнение лабораторных работ позволяет закрепить теоретические знания и получить практические навыки в области информационной безопасности.

СОДЕРЖАНИЕ

Предисловие	3
Лабораторная работа 1. Изучение содержания и последовательности работ по защите информации	4
Лабораторная работа 2. Изучение методов комплексного исследования объекта информатизации	19
Лабораторная работа 3. Изучение информации циркулирующей в корпоративной информационной системе	30
Лабораторная работа 4. Изучение построения системы защиты информации на основе нормативных актов и методических указаний	44
Лабораторная работа 5. Построение модели угроз ИСПДн ...	49
Лабораторная работа 6. Изучение действующей нормативной документации объекта информатизации	61
Лабораторная работа 7. Составление плана мероприятий по улучшению защищённости объекта информатизации	68
Лабораторная работа 8. Разработка политики информационной безопасности	76
Лабораторная работа 9. Исследование методов выбора рационального варианта системы защиты информации на основе экспертной информации	89
Лабораторная работа 10. Исследование методик расчета показателя качества системы защиты информации	102
Лабораторная работа 11. Изучение методов построения комплексной системы организационных и технических мер по защите информации	125
Лабораторная работа 12. Изучение методов построения комплексной защиты сетевой файловой системы	137
Лабораторная работа 13. Комплексная защита электронной почты и документооборота	151
Лабораторная работа 14. Изучение методов построения комплексной защиты сетевых приложений и баз данных	175
Лабораторная работа 15. Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры	201
Лабораторная работа 16. Изучение методов построения комплексной защиты управления информационной безопасностью	214
Лабораторная работа 17. Изучение методики составления испытаний системы защиты информации	234