УДК 004.056.55 (075.8)
ББК 32.973-018 я73
К 82

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

Рецензенты:
д-р техн. наук, профессор Г. И. Линец,
канд. техн. наук, профессор А. Ф. Чипига.

.

К 82 **Криптографические методы защиты информации**: лабораторный практикум / авт.-сост.: И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. – Ставрополь: Изд-во СКФУ, 2015. – 109 с.

Лабораторный практикум подготовлен в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования и представляет собой методические материалы по организации лабораторных работ.

Предназначен для студентов высших учебных заведений, обучающихся по специальности 10.05.03 (090303.65) – Информационная безопасность автоматизированных систем, а также может быть полезен специалистам, интересующимся вопросами правового обеспечения информационной безопасности.

УДК 004.056.55 (075.8)
ББК 32.973-018 я73

Авторы-составители:
д-р техн. наук, профессор И. А. Калмыков,
аспирант кафедры Д. О. Науменко,
аспирант кафедры Т. А. Гиш

ŋqdqɏeY bɆ dǝqɆbYɜǝ d ɐɔɑbɔɏ Ɉqddʎqɏè

ПРЕДИСЛОВИЕ

Дисциплина «Криптографические методы защиты информации» занимается вопросами формирования фундаментальных знаний основных положений теории криптографической защиты информации, оценки криптостойкости, имитостойкости и помехоустойчивости шифров, особенностей использования вычислительной техники в криптографии, привитие умений и навыков использования данных знаний при работе с системами криптографической защиты информации

Задачи дисциплины:

- изучить математические основы криптографических методов защиты информации;
- изучить основные алгоритмы симметричного и асимметричного шифрования данных;
- изучить основы организации структуры криптосистем.

Данная дисциплина базируется на знаниях, полученных студентами в ходе изучения дисциплин: «Информатика», «Дискретная математика», «Теория вероятности и математическая статистка».

Дисциплина «Криптографические методы защиты информации» обеспечивает изучение следующих дисциплин: «Техническая защита информации», «Управление информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности». Знания и практические навыки, полученные из дисциплины «Криптографические методы защиты информации», используются студентами при разработке курсовых и дипломных работ.

Освоение дисциплины позволит будущему специалисту по направлению подготовки 10.05.03 (090303.65) – Информационная безопасность автоматизированных систем полноценно осуществлять свою профессиональную деятельность, в частности, обладать следующими профессиональными компетенциями (ПК):

- способностью применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);
- способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

- способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Лабораторный практикум подготовлен в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования и представляет собой методические материалы по организации лабораторных работ.

УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

При выполнении лабораторной работы ЗАПРЕЩАЕТСЯ:

– самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;

– нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности касаться электрических розеток металлическими предметами и т. д.;

– принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо немедленно сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

ŋqdqɏəɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

СОДЕРЖАНИЕ