УДК 004.056.52 (075.8)
ББК 32.973-018.2 я73
К 63

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

К 63 **Компьютерная криминалистика:** лабораторный практикум / авт.-сост.: И. А. Калмыков, В. С. Пелешенко. – Ставрополь: Изд-во СКФУ, 2017. – 84 с.

Пособие составлено в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, учебным планом и программой дисциплины. Содержит курс лабораторных работ, включающих основные теоретические данные по дисциплине, примеры выполнения работ, задания, литературу.

Предназначено для студентов высших учебных заведений, обучающихся по специальности 10.05.03 (090303.65) – Информационная безопасность автоматизированных систем, а также для преподавателей и специалистов, интересующихся вопросами компьютерной криминалистики.

УДК 004.056.52 (075.8)
ББК 32.973-018.2 я73

Авторы-составители:
д-р техн. наук, профессор *И. А. Калмыков*,
канд. техн. наук, доцент *В. С. Пелешенко*

Рецензенты:
д-р техн. наук, профессор *В. П. Пашинцев*,
д-р техн. наук, доцент *Г. И. Линец*

Содержание

Предисловие

При изучении дисциплины рассматриваются следующие вопросы:

– выработка навыков по обнаружению, оповещению об инцидентах информационной безопасности и их оценке;

– обучение реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий;

– анализ инцидентов информационной безопасности, введение превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

Задачами дисциплины является формирование знаний, позволяющих:

1) обнаруживать события информационной безопасности и эффективно их обрабатывать, а также определять, относятся или не относятся данные события к инцидентам информационной безопасности;

2) давать оценку инцидентам информационной безопасности;

3) минимизировать воздействие инцидентов информационной безопасности на защищенные автоматизированные системы управления.

В процессе обучения формируются следующие компетенции:

– ПК-4 – способность понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;

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

– ПК-24 – способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем;

– ПК-25 – способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизи-

ŋqqdʎǝʎ bƎ dǝdƎbʎɜǝ d ɛɔɑbɔʎ Ɉqqdʎqʎè

рованных систем с учетом нормативных требований по защите информации;

– ПК-30 – способность организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности.

Для выполнения лабораторных работ потребуются следующие *оборудование и материалы:*

– аппаратура: персональный компьютер со следующими характеристиками: процессор Pentium/Celeron с тактовой частотой 300 МГц и выше, оперативная память – не менее 128 Мбайт и более, свободное дисковое пространство – не менее 100 MB Мбайт, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 256);

– программное обеспечение: операционная система WINDOWS 2000/ XP Professional, библиотека Microsoft .NET Framework версии 1.1 или выше, программа Mathcad 13 и выше.

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).