УДК 004.56(06) (075.8)
ББК 32.973.26-018.2 я73
П 29

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

Рецензенты:
доктор физико-математических наук, доцент Ф. Б. Тебуева,
кандидат технических наук, доцент В. Е. Рачков

Петренко В. И.
П 29 **Теоретические основы защиты информации:** учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

Пособие соответствует федеральному государственному образовательному стандарту высшего образования по данному направлению. В нем раскрыты основные методологические принципы формирования защиты информации, описаны стратегии защиты информации. Понятийный аппарат пособия изложен в соответствии с принятой научной терминологией в области информационной безопасности на основе действующей нормативной базы.

Предназначено для студентов, обучающихся по направлению 10.03.01 – Информационная безопасность.

УДК 004.56(06) (075.8)
ББК 32.973.26-018.2 я73

ŋqdqɣɐɤ ɓƷ ɗəpƷɓɤɜɐ ɗ ɛɔɑɓɔɤ Ɉqdqɤqɣè

ВВЕДЕНИЕ

Информационные технологии испытывают постоянный бурный рост. В последнее время наблюдается особенно стремительное их развитие, проявляющееся в регулярном появлении новых и модернизации старых программных и аппаратных средств. В свою очередь, такой бурный рост сопряжён с появлением новых уязвимостей в продуктах информационных технологий и новых угроз информационной безопасности. Для построения эффективных решений в области систем защиты информации требуются глубокие знания теории защиты информации.

Теория защиты информации определяется как система основных идей, относящихся к защите информации в современных системах ее обработки, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

В данном пособии раскрыты основные методологические принципы формирования защиты информации, описаны стратегии защиты информации. Пособие состоит из 14 глав.

В первой главе приведены основные свойства информации как предмета защиты, дано определение информации, сформулированы свойства меры количества информации и энтропии.

Во второй главе раскрыто современное состояние защиты информации, ретроспектива и перспектива защиты информации, приведены понятия информационной системы, канала и сети передачи.

В третьей главе даны определения и основные понятия теории защиты информации, раскрыты общеметодологические принципы формирования теории защиты информации, приведены стратегии защиты информации.

В четвертой главе дана классификация угроз информационной безопасности, описаны случайные и преднамеренные угрозы, приведены угрозы безопасности информационных и телекоммуника-

ŋqdqуеҮ bɆ dеdɆbҮзе d ɛɑɑbɑу ɈqdqҮqуè

ционных средств и систем, описаны цели и механизмы реализации информационных атак.

В пятой главе детально рассмотрен процесс разработки политики безопасности, приведено формальное и неформальное описание политики безопасности.

В шестой главе рассмотрены основные модели безопасности, описывающие дискреционный (произвольный) контроль и управление доступом, а также механизмы, которые необходимо реализовать в вычислительных системах для его поддержки.

В седьмой главе основное внимание уделяется определению условий, при которых в системе возможно распространение прав доступа с использованием модели Take-Grant, а также рассмотрены условия реализации способа санкционированного получения прав доступа и способа похищения прав доступа.

В восьмой главе рассмотрены основные модели безопасности, описывающие мандатный (нормативный) контроль доступом, а также механизмы, которые необходимо реализовать в вычислительных системах для его поддержки.

В девятой главе рассмотрены вопросы реализации различных моделей контроля целостности, приведен их сравнительный анализ, а также рассмотрены их достоинства и недостатки.

В десятой главе рассмотрены основные ролевые модели доступа. Контроль доступа, базирующийся на ролях (role based access control) (КДБР), рассматривает всю информацию, обрабатывающуюся в вычислительной системе организации, как принадлежащую данной организации.

В одиннадцатой главе подробно рассмотрены такие основные методы аутентификации как: аутентификация, основанная на обладании предметом; аутентификация, основанная на воплощенных характеристиках и аутентификация, основанная на знании.

В двенадцатой главе сформулированы требования к подсистемам аудита, показан пример реализации подсистемы аудита в операционной системе Windows и рассмотрены основные вопросы реализации аудита информационной безопасности предприятия.

Тринадцатая глава посвящена описанию уязвимостей информационных систем, ошибок, приводящих к уязвимостям, технике

поиска уязвимостей в процессе разработки, анализа и функционирования систем.

В четырнадцатой главе приведены основные схемы реализации атак и простейших сценариев вторжения, а также рассмотрено в качестве примера современных средств атак использование компьютерных вирусов и червей.

ОГЛАВЛЕНИЕ