

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

© ФГАОУ ВПО «Северо-Кавказский
федеральный университет», 2015

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-

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, обрабатываемую 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

ВВЕДЕНИЕ.....	3
1. ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ КАК ПРЕДМЕТА ЗАЩИТЫ.....	6
1.1. Количество информации.....	6
1.2. Основные свойства информации, влияющие на возможность ее защиты.....	10
2. ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ.....	25
2.1. Современное состояние защиты информации, перспектива и ретроспектива.....	25
2.2. Информационные системы, средства, каналы, сети и среды.....	42
3. ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ.....	48
3.1. Определение и основные понятия теории защиты информации.....	48
3.2. Общеметодологические принципы формирования теории защиты информации.....	50
3.3. Стратегии защиты информации.....	54
4. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.....	62
4.1. Информационные угрозы.....	62
4.2. Информационные атаки.....	69
5. ПОЛИТИКА БЕЗОПАСНОСТИ.....	72
5.1. Процесс разработки политики.....	73
5.2. Неформальное описание политики безопасности.....	77
5.3. Формальное описание политики безопасности.....	84
6. ДИСКРЕЦИОННЫЙ КОНТРОЛЬ И УПРАВЛЕНИЕ ДОСТУПОМ.....	88
6.1. Матрица доступа.....	88
6.2. Модель Харрисона, Руззо и Ульмана.....	90

6.3. Модель распространения прав доступа TAKE-GRANT	94
7. МОДЕЛЬ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА TAKE-GRANT	99
7.1. Санкционированное получение прав доступа	99
7.2. Похищение прав доступа	102
7.3. Расширенная модель Take-Grant	103
8. МОДЕЛИ МАНДАТНОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ	109
8.1. Уровни секретности	109
8.2. Модель Белла и Лападула	111
8.3. Критика модели Белла и Лападула	114
9. МОДЕЛИ КОНТРОЛЯ ЦЕЛОСТНОСТИ	120
9.1. Модель Биба	120
9.2. Модель Кларка–Вилсона	124
9.3. Объединение моделей безопасности	127
9.3.1. Объединение модели Белла и Лападула и модели Биба	128
9.3.2. Объединение моделей Кларка–Вилсона и Биба	131
9.3.3. Модель Липнера	131
9.3.4. Модель Липнера на основе модели Белла и Лападула и Биба	135
10. РОЛЕВЫЕ МОДЕЛИ ДОСТУПА	138
10.1. Пользователи, роли и операции	139
10.2. Роли и иерархия ролей	141
10.3. Авторизация и активация роли	142
10.4. Операционное разделение обязанностей и доступ к объектам	145
11. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ	148
11.1. Роль и задачи аутентификации	149
11.2. Парольная аутентификация	153
11.3. Биометрическая аутентификация	158

11.4. Аутентификация, основанная на обладании предметом.....	163
12. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	172
12.1. Требования к подсистеме аудита.....	173
12.2. Реализация подсистемы аудита в операционной системе Windows.....	176
12.3. Аудит информационной безопасности предприятия...	177
13. УЯЗВИМОСТИ.....	183
13.1. Основные определения.....	183
13.2. Ошибки, приводящие к уязвимостям.....	186
13.3. Поиск уязвимостей в процессе разработки и анализа систем.....	191
13.4. Поиск уязвимостей в процессе функционирования систем.....	197
14. АТАКИ И ВТОРЖЕНИЯ.....	200
14.1. Характеристики атак.....	200
14.2. Вторжения.....	202
14.3. Компьютерные вирусы и черви.....	207
ЛИТЕРАТУРА.....	214
ГЛОССАРИЙ.....	216
СПИСОК СОКРАЩЕНИЙ.....	218