УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
П82

Проскурин В. Г.

П82 Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.: ил.

ISBN 978-5-9912-0379-1.

Подробно рассмотрены основные средства и методы обеспечения информационной безопасности в современных операционных системах: управление доступом, аутентификация, аудит и обнаружение вторжений. Кроме того, отдельно рассматриваются некоторые специфические вопросы, косвенно связанные с обеспечением безопасности операционных систем: централизованное управление политиками безопасности в доменах Windows, особенности обеспечения безопасности операционных систем мобильных устройств, концепция виртуализации операционных систем и ее влияние на информационную безопасность. Изложение теоретического материала иллюстрируется практическими примерами. В конце каждой главы приведен перечень вопросов для самопроверки, в конце пособия – методические рекомендации по его изучению.

Для студентов (слушателей) вузов, обучающихся по специальностям 10.05.01 – «Компьютерная безопасность», 10.05.03 – «Информационная безопасность автоматизированных систем» и 10.05.04 – «Информационно-аналитические системы безопасности», по направлению подготовки 10.03.01 – «Информационная безопасность», уровень бакалавр.

ББК 32.973.2-018.2я73

Адрес издательства в Интернет WWW.TECHBOOK.RU

Учебное издание

Проскурин Вадим Геннадьевич

ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника О. В. Карповой

Подписано в печать 25.12.2013. Формат 60×88/16. Уч. изд. л. 12. Тираж 500 экз.
ООО «Научно-техническое издательство «Горячая линия – Телеком»

ISBN 978-5-9912-0379-1

ŋqdpʎɐʎ pƎ dɐdƎbʎɜɐ p ɐɔɐbɔʎ Ɉqddʎqʎè

Оглавление

Предисловие 3

1 Понятие защищенной операционной системы 4

1.1. Основные определения 4
1.2. Основные подходы к построению защищенных операционных систем 4
1.3. Административные меры защиты 6
1.4. Адекватная политика безопасности 6
1.5. Стандарты безопасности операционных систем 10
Вопросы для самопроверки 15

2 Управление доступом 14

2.1. Основные определения 14
2.2. Типовые модели управления доступом 19
2.3. Управление доступом в Windows 26
2.4. Управление доступом в UNIX 62
Вопросы для самопроверки 69

3 Аутентификация 72

3.1. Общие сведения 72
3.2. Аутентификация в UNIX 92
3.3. Аутентификация в Windows 99
Вопросы для самопроверки 108

4 Аудит и обнаружение вторжений 110

4.1. Общие сведения 110
4.2. Системы обнаружения вторжений 114
4.3. Аудит в Windows 120
4.4. Аудит в UNIX 124
Вопросы для самопроверки 132

5 Домены Windows 134

5.1. Общие сведения 134
5.2. Сквозная аутентификация 135
5.3. Отношения доверия 139
5.4. Активный каталог 141
5.5. Групповая политика 149
Вопросы для самопроверки 155

6 Безопасность операционных систем мобильных устройств 157
Вопросы для самопроверки 165
7 Виртуализация операционных систем 169
Вопросы для самопроверки 180
Приложение. Методические рекомендации по организации изучения дисциплины «Защита в операционных системах» 182
Анализ требований ФГОС ВПО 182
Организация изучения дисциплины «Защита в операционных системах» 186
Литература 189