

Предисловие
Глава 1. Общие положения
Предмет и задачи теории защиты информации
Базовые термины и определения
Глава 2. Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки.
Понятие надежности безопасности
Классификация угроз безопасности
Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характеристики безопасности
Классификация угроз уязвимостей и уровней защиты (защищенности)
Объекты защиты и объекты моделирования
Вопросы и задания для самоконтроля
Глава 3. Методы и абстрактные модели защиты информации
Основополагающие методы и абстрактные модели контроля доступа
Метод и абстрактная модель дискреционного контроля доступа
Альтернативный метод и абстрактная модель избирательного контроля доступа
Метод и абстрактная модель мандатного контроля доступа
Методы и абстрактные модели контроля доступа к создаваемым объектам
Вероятностная и процессная модели контроля доступа
Абстрактные модели контроля доступа к защищенным режимам обработки информации
Модели и методы ролевого и сессионного контроля доступа.
Вопросы идентификации ролей и сессий
Задачи построения системы защиты информации
Основная и дополнительная задачи системы защиты информации.
Задача обеспечения корректной реализации базового уровня защиты
Задача обеспечения корректной реализации повышенного уровня защиты
Альтернативные методы защиты информации
Вопросы и задания для самоконтроля
Глава 4. Исходные данные и общий подход к математическому моделированию угроз безопасности Моделирование уязвимостей реализации и атак.
Исходные данные для моделирования угроз безопасности
Определение требований к качеству разработки и технического сопровождения системы защиты информации
Экономическое обоснование проектных решений
Оценка производительности системы защиты информации
Эксплуатационное проектирование системы защиты информации
Вопросы и задания для самоконтроля
Литература
Новинки по дисциплине