Аннотация рабочей программы дисциплины

«Модели конфиденциальности, целостности и доступности информации»

Направление подготовки

09.03.02. Информационные системы и технологии

Направленность (профиль) образовательной программы

Безопасность информационных систем

Содержание дисциплины

№	Содержание раздела
Раздел 1	Задачи абстрактных моделей безопасности, основные понятия. Абстрактная модель безопасности (АМБ) Харрисона, Руссо, Ульмана (ХРУ). Формальное описание АМБ ХРУ. Определение безопасного состояния. Примеры реализации.
Раздел 2	Анализ безопасности АМБ ХРУ. Доказательство разрешимости монооперационной АМБ ХРУ. Доказательство неразрешимости АМБ ХРУ в общем виде. Монотонная АМБ ХРУ
Раздел 3	АМБ Типизированная матрица доступов (ТМД). Формальное описание АМБ ТМД. Представление АМБ ТМД в виде АМБ ХРУ. АМБ Монотонная типизированная матрица доступов (МТМД). Каноническая форма АМБ МТМД (КФМТМД). Теорема об эквивалентности АМБ МТМД некоторой АМБ КФМТМД. Определение дочерних и родительских типов. Граф создания. Ациклическая МТМД (АМТМД) и КФМТМД (АКФМТМД). Определение отношения частичного строгого порядка на множестве команд АМТМД. Лемма о свойствах антисимметричности, антирефлексивности и транзитивности. Алгоритм построения развернутого состояния для АКФМТМД. Теорема о существовании алгоритма проверки АМТМД. Следствие о сложности алгоритма проверки. Тернарная АМТМД, сложность алгоритма проверки.
Раздел 4	Классическая АМБ take-grant. Формальное описание АМБ take-grant. ”. Остров, мост, начальный пролет моста, конечный пролет моста. Теорема о необходимых и достаточных условиях истинности предиката “возможен доступ”. Похищение права доступа. Теорема о необходимых и достаточных условиях истинности предиката “возможно похищение”.
Раздел 5	Расширенная АМБ take-grant.Де-факто правила расширенной модели take-grant. Определение предиката “возможна запись”. Теорема о необходимых и достаточных условиях истинности предиката “возможна запись”. Построение замыкания графа доступов и информационных потоков. Анализ путей распространения прав доступа и информационных потоков. Представление модели take-grant моделью ХРУ.
Раздел 6	АМБ Белла-ЛаПадулы. Понятие решетки. Классическая модель Белла-ЛаПадулы. Модель Read-Write. Безопасность переходов. Политика loe watermark в модели Белла-ЛаПадулы.
Раздел 7	Модель целостности Биба. Формальное описание классической модели Биба. Политика Low-watermark для субъектов. . Политика Low-watermark для объектов. . Политика Low-watermark при неизменных значениях функций Is, Io.
Раздел 8	Криптография. Основные определения. Классификация и сравнительная характеристика современных криптоалгоритмов. Конечное поле Fp. Быстрое вычисление инверсии с помощью расширенного алгоритма Евклида.
Раздел 9	Современные симметричные блочные шифры. Конструирование S-Рсети. Сеть Фейстеля. SDES. DES. Российский стандарт ГОСТ 28147-89- ГОСТ 34.12-2018 (Магма). IDEA. Недостатки DES. Модификации DES.

Раздел 10	Вычисление инверсии в конечном поле F_2^p с помощью расширенного алгоритма Евклида для F_2^p. Алгоритм SAES. Стандарт шифрования AES. Операции Subbyte, MixColumns. Стандарт шифрования ГОСТ 34.12-2018 (Кузнечик).
Раздел 11	Режимы шифрования блочных шифров. Шифрование “хвостов”.

Практическая подготовка при изучении дисциплины реализуется непосредственно в университете.