Модели безопасности компьютерных систем.

Примерные вопросы к экзамену

1. Введение в МБКС.
   1. Основные понятия МБКС. Подход к формальному описанию «пользователей». Основная аксиома МБКС.
   2. Модели ценности информации.
2. Виды политик безопасности.
   1. Дискреционная политика безопасности. Определение и примеры.
   2. Мандатная политика безопасности. Определение и примеры.
   3. Политика ролевого разграничения доступа. Определение и примеры.
   4. Политика безопасности информационных потоков. Определение и примеры.
   5. Политика изолированной программной среды.
3. Модели безопасности КС.
   1. Модели на основе дискреционного разграничения доступа.
      1. Модель take-grant.
         1. Классическая модель take-grant. Основные понятия и правила. Предикат «возможен доступ». Частный случай эквивалентных условий. Теорема 1(без док-ва).
         2. Классическая модель take-grant. Определение моста, острова, конечного и начального пролетов моста. Теорема 2. (без док-ва).
         3. Вопрос похищения прав доступа.
      2. Расширенная модель take-grant.
         1. Де-факто и де-юре правила. Предикат «возможна запись». Теорема 4 (без док-ва).
         2. Построение замыкания графа доступов и информационных потоков. Вопрос «стоимости» или вероятности использования путей для передачи прав доступа или реализации информационных потоков.
      3. Модель Харрисона-Руззо-Ульмана (ХРУ).
         1. Основные понятия, примитивные операторы и команды.
         2. Анализ безопасности систем ХРУ.
            1. Алгоритмическая проверка безопасности монооперационной системы ХРУ.
            2. Гомоморфизм Машины Тьюринга в ХРУ.
            3. Представление модели take-grant через систему ХРУ.
            4. Вопрос утечки прав доступа в конкретную ячейку.
   2. Модели мандатного разграничения доступа.
      1. Модель Белла-Ла-Падулы.
         1. Классическая модель БЛаП. Основные определения. Виды запросов. Свойства безопасности в модели БЛаП.
         2. Безопасность базовой модели БЛаП. Теоремы А1,А2,А3,БТБ(без док-ва).
         3. Пример некорректного определения свойств безопасности.
         4. Безопасность переходов БЛаП. Теоремы А1-RW, A2-RW, БТБ-RW(без док-ва).
   3. Изолированная программная среда.
   4. Модель ролевого разграничения и управления доступом.
      1. Основные понятия и определения.
      2. Модель административного ролевого управления доступом.
4. Документы по сертификации компьютерных систем.
   1. «Оранжевая книга». (TCSEC).
   2. Европейские критерии. (ITSEC).
   3. ГОСТ Р 15408
5. Обзор OS AstraLinux.

Билет 1

1. Введение в МБКС. **Основные понятия МБКС. Подход к формальному описанию «пользователей». Основная аксиома МБКС.**
2. Обзор OS AstraLinux.

Билет 2

1. Введение в МБКС. **Модели ценности информации.**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **Европейские критерии. (ITSEC).**

Билет 3

1. Виды политик безопасности. **Дискреционная политика безопасности. Определение и примеры.**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **«Оранжевая книга». (TCSEC).**

Билет 4

1. Виды политик безопасности. **Мандатная политика безопасности. Определение и примеры.**
2. Реализация моделей безопасности КС. Модель ролевого разграничения и управления доступом. **Модель административного ролевого управления доступом.**

Билет 5

1. Виды политик безопасности. **Политика ролевого разграничения доступа. Определение и примеры.**
2. Реализация моделей безопасности КС. **Модель ролевого разграничения и управления доступом. Основные понятия и определения.**

Билет 6

* + - 1. Виды политик безопасности. **Политика безопасности информационных потоков. Определение и примеры.**
      2. Реализация моделей безопасности КС. **Изолированная программная среда.**

Билет 7

1. Виды политик безопасности. **Политика изолированной программной среды.**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. **Модель Белла-Ла-Падулы. Безопасность переходов БЛаП. Теоремы А1-RW, A2-RW, БТБ-RW(без док-ва).**

Билет 8

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Классическая модель take-grant. Основные понятия и правила. Предикат «возможен доступ». Частный случай эквивалентных условий. Теорема 1(без док-ва).**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. **Модель Белла-Ла-Падулы. Пример некорректного определения свойств безопасности.**

Билет 9

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Классическая модель take-grant. Определение моста, острова, конечного и начального пролетов моста. Теорема 2. (без док-ва).**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа**. Модель Белла-Ла-Падулы. Безопасность базовой модели БЛаП. Теоремы А1,А2,А3,БТБ(без док-ва).**

Билет 10

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Вопрос похищения прав доступа.**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. Модель Белла-Ла-Падулы. **Классическая модель БЛаП. Основные определения. Виды запросов. Свойства безопасности в модели БЛаП.**

Билет 11

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Расширенная модель take-grant. Де-факто и де-юре правила. Предикат «возможна запись». Теорема 4 (без док-ва).**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Вопрос утечки прав доступа в конкретную ячейку.**

Билет 12

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Расширенная модель take-grant. Построение замыкания графа доступов и информационных потоков. Вопрос «стоимости» или вероятности использования путей для передачи прав доступа или реализации информационных потоков.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Представление модели take-grant через систему ХРУ.**

Билет 13

1. Виды политик безопасности. **Политика изолированной программной среды.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Основные понятия, примитивные операторы и команды.**

Билет 14

1. Введение в МБКС. **Модели ценности информации.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Алгоритмическая проверка безопасности монооперационной системы ХРУ.**

Билет 15

1. Введение в МБКС. **Основные понятия МБКС. Подход к формальному описанию «пользователей». Основная аксиома МБКС.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Гомоморфизм Машины Тьюринга в ХРУ.**

Билет 16

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant Классическая модель take-grant. Основные понятия и правила. Предикат «возможен доступ». Частный случай эквивалентных условий. Теорема 1(без док-ва).**
2. **Обзор OS AstraLinux.**

Билет 17

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Классическая модель take-grant. Определение моста, острова, конечного и начального пролетов моста. Теорема 2. (без док-ва).**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **Европейские критерии. (ITSEC).**

Билет 18

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Вопрос похищения прав доступа.**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **«Оранжевая книга». (TCSEC).**

Билет 19

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Расширенная модель take-grant. Де-факто и де-юре правила. Предикат «возможна запись». Теорема 4 (без док-ва).**
2. Реализация моделей безопасности КС. **Модель ролевого разграничения и управления доступом. Модель административного ролевого управления доступом.**

Билет 20

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Расширенная модель take-grant. Построение замыкания графа доступов и информационных потоков. Вопрос «стоимости» или вероятности использования путей для передачи прав доступа или реализации информационных потоков.**
2. Реализация моделей безопасности КС. **Модель ролевого разграничения и управления доступом. Основные понятия и определения.**

Билет 21

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Основные понятия, примитивные операторы и команды.**
2. Реализация моделей безопасности КС. **Изолированная программная среда.**

Билет 22

1. Виды политик безопасности. **Дискреционная политика безопасности. Определение и примеры.**
2. Модели мандатного разграничения доступа. Модель Белла-Ла-Падулы. **Классическая модель БЛаП. Основные определения. Виды запросов. Свойства безопасности в модели БЛаП.**

Билет 23

1. Виды политик безопасности. **Мандатная политика безопасности. Определение и примеры.**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. **Модель Белла-Ла-Падулы. Безопасность базовой модели БЛаП. Теоремы А1,А2,А3,БТБ(без док-ва).**

Билет 24

1. Виды политик безопасности. **Политика ролевого разграничения доступа. Определение и примеры.**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. **Модель Белла-Ла-Падулы. Пример некорректного определения свойств безопасности.**

Билет 25

1. Виды политик безопасности. **Политика безопасности информационных потоков. Определение и примеры.**
2. Реализация моделей безопасности КС. Модели мандатного разграничения доступа. **Модель Белла-Ла-Падулы. Безопасность переходов БЛаП. Теоремы А1-RW, A2-RW, БТБ-RW(без док-ва).**

Билет 26

1. Виды политик безопасности. **Политика изолированной программной среды.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Алгоритмическая проверка безопасности монооперационной системы ХРУ.**

Билет 27

1. Введение в МБКС. **Основные понятия МБКС. Подход к формальному описанию «пользователей». Основная аксиома МБКС.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Гомоморфизм Машины Тьюринга в ХРУ.**

Билет 28

1. Введение в МБКС. **Модели ценности информации.**
2. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Представление модели take-grant через систему ХРУ.**

Билет 29

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Модель take-grant. Модель Харрисона-Руззо-Ульмана(ХРУ). Анализ безопасности систем ХРУ. Вопрос утечки прав доступа в конкретную ячейку.**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **«Оранжевая книга». (TCSEC).**

Билет 30

1. Реализация моделей безопасности КС. Модели на основе дискреционного разграничения доступа. **Расширенная модель take-grant. Де-факто и де-юре правила. Предикат «возможна запись». Теорема 4 (без док-ва).**
2. Исторические зарубежные нормативные документы по сертификации компьютерных систем. **Европейские критерии. (ITSEC).**