Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Модели безопасности компьютерных систем

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-11.1 Понимает основные формальные модели политик управления доступом и информационными потоками в компьютерных системах

ИОПК-11.2 Владеет необходимым аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах

ИОПК-11.3 Формулирует политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

ИОПК-8.3 Проводит анализ и формализацию поставленных задач, участвует в разработке математических моделей в области обеспечения безопасности компьютерных систем и сетей

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– контрольная работа;

– лабораторный проект;

– доклад.

Контрольная работа состоит из двух частей, теоретического вопроса, на который необходимо дать ответ (раскрыть понятие, описать алгоритм и т.д.), и задачи. Для каждой темы курса предусмотрено несколько вопросов и задач.

Тема 1. Основные элементы и виды управления доступом (ИОПК-11.1, ИОПК-8.3, ИОПК-11.3, ИПК-2.1)

Примеры задач.

Отобразить граф доступов с информационным потоком, реализуемом при кооперации двух субъектов.

Ответ должен содержать граф доступов с не менее чем двумя субъектами и тремя объектами, между которыми субъекты реализуют передачу с использованием доступов read и write. Например для трёх субъектов, *a*, *b* и *c*. Один субъект должен иметь доступ write к *b* и read к *a*, а второй, write к *c* и read к *b*.

Привести пример субъектов и объектов в реальных компьютерных системах.

Ответом может быть ОС, где субъектам соответствуют пользователи и запускаемые процессы. В качестве объектов выступают файлы, в том числе папки.

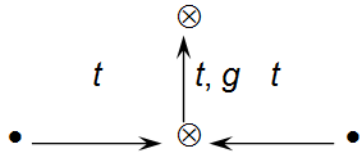
Теоретические вопросы.

1. Политика безопасности и механизм управления доступом

2. Сущность, объект, субъект, контейнер
3. Права доступа и доступы
4. Информационные потоки по памяти и времени
5. Монитор безопасности
6. Три аксиомы компьютерной безопасности

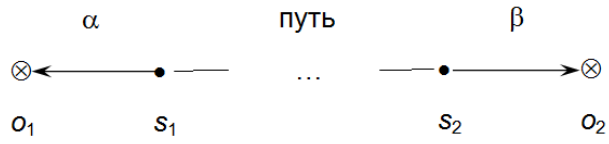
Тема 2. Take-Grant модель (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1-2)
Примеры задач.

1. Является ли граф доступов мостом.



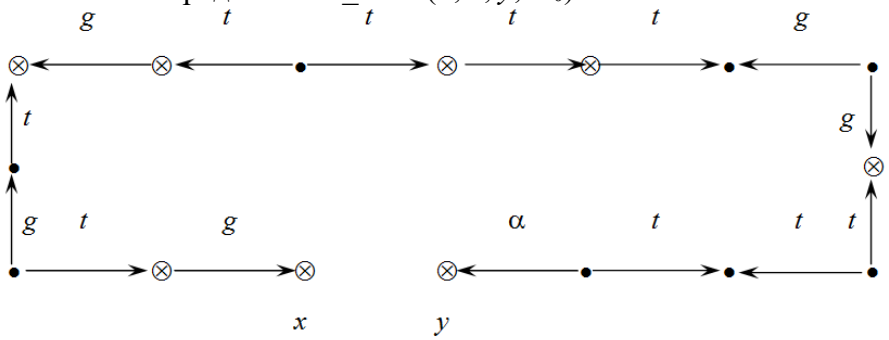
Ответ: да.

2. Пусть возможна передача прав доступа в одну сторону. Возможна ли она в противоположную сторону?



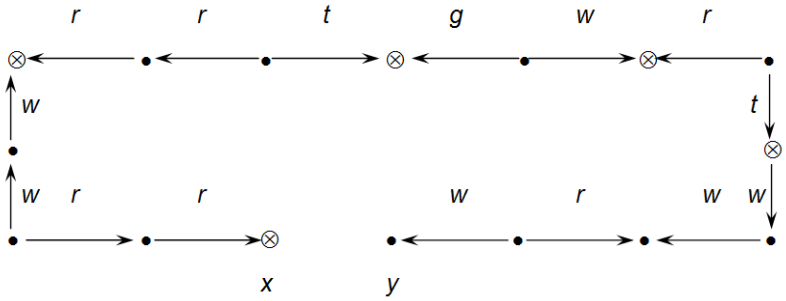
Ответ: да, в ответе необходимо продемонстрировать механизм передачи.

3. Истинен ли предикат can_share(α, *x*, *y*, G_0)?



Ответ: да, в ответе необходимо достроить все недостающие права, которые могут быть переданы.

4. Истинен ли предикат can_write(*x*, *y*, G_0)?



Ответ: да, в ответе необходимо достроить все недостающие права и информационные потоки.

Теоретические вопросы.

1. Модель контроля доступа как автомат, траектория функционирования КС
2. Описание take-grant модели, де-юре правила

3. Предикат can_share и условия передачи прав доступа для графа доступов, включающего только субъекты
4. Условия передачи прав доступа для произвольного графа доступов (мосты и острова)
5. Условия похищения прав доступа
6. Скрытые (неявные) информационные потоки
7. Описание расширенной take-grant модели, де-факто правила
8. Условия информационного потока и истинности предиката can_write
9. Замыкание модели (tg-замыкание, де-юре замыкание, де-факто замыкание

Тема 3. Ролевая модель (ИОПК-11.1-3, ИПК-2.1-2)

Примеры задач.

Привести пример ролевой системы контроля доступа с

1. иерархией ролей
2. ограничением взаимного исключения ролей или прав доступа
3. количественным ограничением на обладание ролью или правом доступа
4. ограничением необходимого обладания ролью или правом доступа

Ответ может быть дан в форме рисунка или текстового описания и должен содержать указанный механизм.

Теоретические вопросы.

1. Определение ролевой модели управления доступом
2. Критерий безопасности для базовой ролевой модели и иерархии ролей
3. Механизмы ограничений ролевой модели
4. Административные роли

Тема 4. Модель изолированной программной среды и основы ДП моделей (ИОПК-11.1-2, ИПК-2.1)

Примеры задач.

Привести пример ассоциированных объектов в реальных компьютерных системах.

Ответами могут быть процессы ОС, функционирование которых зависит от информации из файлов. Монитор безопасности и ассоциированные с ним списки доступа, антивирус и его БД.

Теоретические вопросы.

1. Основные элементы модели ИПС
2. Ассоциированные объекты
3. МБО
4. Корректность субъектов
5. МБС
6. Базовая теорема ИПС
7. Ядро безопасности и создание гарантированно защищенной КС
8. Базовая ДП-модель

Тема 5. Модели Белла-ЛаПадулы и Биба (ИОПК-8.3, ИОПК-11.1-3, ИПК-2.2)

Примеры задач.

1. Нарисовать граф доступов, нарушающий ss-свойство

   Ответом является граф доступа, где субъект обладает доступом на чтение объекта большего уровня, чем субъект.
2. Нарисовать граф доступов, нарушающий *-свойство

Ответом является граф доступа, где субъект обладает доступом на запись в объект меньшего уровня, чем субъект.

3. Дана система $S = \{s_1, s_2\}$, $O = \{o_1, o_2\}$, $R = \{read, write\}$, $(L, \leq) = (Low, High)$ $f_s(s_1) = f_o(o_1) = Low$, $f_s(s_2) = f_o(o_2) = High$. Подсчитать количество состояний для следующих случаев:
    A. не требуется выполнение свойств безопасности
    B. выполняется simple security свойство (Какие запрещённые потоки могут быть реализованы в данном случае?)
    C. выполняется simple security свойство и * свойство (Остались ли запрещённые потоки с прежнего пункта?)

Ответы:
A.
56
B.
4
C.

Теоретические вопросы.

1. Основные элементы модели BLP, виды запросов
2. Свойства безопасности (ss-свойство, *-свойство, ds-свойство)
3. Теоремы безопасности и их доказательства
4. Политика low-watermark
5. Проблема последовательности переходов, функция переходов и уполномоченные субъекты
6. Модель целостности Биба

Тема 6. Разработка механизмов управления доступом для современных компьютерных систем (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

Примеры задач.

Привести пример системы, работающей по механизму

1. Списков или матрицы доступа
2. Ролей
3. Решёток уровней конфиденциальности
4. Тематического ограничения доступа
5. Атрибутного контроля доступа

Ответ может быть дан в форме рисунка или текстового описания и должен содержать указанный механизм

Теоретические вопросы.

1. Дискреционная и мандатная политика
2. Матрица доступа
3. Уровни конфиденциальности и тематические метки
4. Ролевой контроль доступа
5. Атрибутный механизм контроля доступа

Критерии оценивания контрольных работ:

Результаты контрольной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если дан верный ответ на теоретический вопрос и задача решена правильно.

Оценка «хорошо» выставляется, если либо в ответе на вопрос была допущена неточность, либо при решении задачи была допущена техническая ошибка, несмотря на верный алгоритм решения.

Оценка «удовлетворительно» выставляется, если в ответе на вопрос была допущена неточность и при решении задачи была допущена техническая ошибка, несмотря на верный алгоритм решения.

Оценка «неудовлетворительно» выставляется, если ответ на теоретический вопрос не дан, дан неверно, или задача решена неправильно.

Доклад (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

Доклад демонстрируется на практических занятиях. Время на доклад: 10 минут. При большом объёме материала допускается наличие нескольких непересекающихся докладов по одной теме.

Примерный список тем

1. Модель ХРУ (теоремы о алгоритмической неразрешимости проверки безопасности с доказательством)
2. Модель типизированной матрицы доступов
3. Необходимые и достаточности истинности предикатов can_write_memory и can_write_time для базовой ДП модели
4. ДП-модель для политики безопасности администрирования. Разделение административных и пользовательских полномочий
5. Модель системы военных сообщений СВС
6. Вероятностная и программная модели контроля потоков
7. Модель администрирования ролевого управления доступом
8. Ролевая ДП-модель
9. Тематическое разграничения доступа (TBAC)
10. Ограничение доступа на основе атрибутов (теоретические основы)
11. Дискреционный контроль доступа в операционных системах.
12. SELinux
13. XACML и его реализации
14. Реализация политики безопасности в облачных хранилищах
15. Реализации контроля доступа в СУБД
16. AppArmor
17. Средства мандатного контроля доступа в ОС
18. Система контроля доступа на конкретном примере

В случае успешной защиты, ставится оценка зачтено.

Групповой проект (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

Цель: реализовать механизм управления доступом для выбранной компьютерной системы (КС).

Этапы выполнения.

1. Выбрать КС для разработки и реализации (можно взять существующую).
2. Построить и обосновать модель безопасности для заданной системы.
3. Разработать и реализовать выбранную компьютерную систему и механизм контроля доступа.

Варианты реализации:

1. Контроль доступа в СУБД
2. Веб-приложение/сайт с контролем доступа пользователей
3. Файловый менеджер
4. Другие варианты после обсуждения с преподавателем

Требования к реализации

1) Для механизмов на основе матрицы доступов: возможность передачи прав на основе “владения” или других административных прав.

2) Для механизмов на основе уровней/меток конфиденциальности: наличие не менее трёх уровней/тематик или возможность добавлять новые уровни/тематики; запрет на чтение вверх (более широкой тематики) и запись вниз (в меньшую тематику).

3) Для механизмов на основе ролей: наличие не менее трёх ролей; реализация хотя бы одного из механизмов ограничений или иерархии ролей.

4) Для механизмов на основе атрибутов: наличие хотя бы по одному атрибуту субъектов, объектов, доступа и среды; каждый атрибут должен присутствовать хотя бы в одном предикате.

5) Для всех: возможность добавлять субъекты и объекты; наличие системы аутентификации.

В ходе реализации практического задание допускается использование любых средств, находящихся в открытом доступе.

Допускаются группы от одного до трёх человек.

Лабораторный проект защищается с презентацией на практических занятиях и, в случае выполнения всех требований, ставится оценка «зачтено». Если система контроля доступа функционирует, но одно из требований не выполнено, то ставится оценка «условно зачтено». В противном случае – ставится оценка «не зачтено».

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзаменационный билет состоит из трех вопросов по разным темам курса. Покрытие вопросами образовательных результатов аналогично таковому для текущего контроля (раздел 2). **Тема 1. Основные элементы и виды управления доступом** (ИОПК-11.1, ИОПК-8.3, ИОПК-11.3, ИПК-2.1). **Тема 2. Take-Grant модель** (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1-2). **Тема 3. Ролевая модель** (ИОПК-11.1-3, ИПК-2.1-2). **Тема 4. Модель изолированной программной среды и основы ДП моделей** (ИОПК-11.1-2, ИПК-2.1). **Тема 5. Модели Белла-ЛаПадулы и Биба** (ИОПК-8.3, ИОПК-11.1-3, ИПК-2.2). **Тема 6. Разработка механизмов управления доступом для современных компьютерных систем** (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1).

Перечень теоретических вопросов.

1. Базовая терминология (сущность, объект, субъект, контейнер), доступы, информационные потоки по памяти и времени.
2. Свойства безопасности модели BLP (simple security-свойство, *-свойство, ds-свойство). Теоремы безопасности и их доказательства.
3. Три аксиомы компьютерной безопасности.
4. Замыкание расширенной take-grant модели.
5. Дискреционная и мандатная политики. Основные признаки, преимущества и недостатки.
6. ИПС: МБО и МБС, Базовая теорема ИПС, Ядро безопасности и создание гарантированно защищенной КС.
7. Особенности и принципы ролевой модели управления доступом, иерархия ролей и критерии безопасности.
8. Формальное определение и основные элементы базовой ДП модели, условия передачи прав доступа.
9. Условия передачи прав доступа для произвольного графа доступов в базовой модели take-grant (мосты и острова), условия похищения прав доступа.
10. Основные элементы модели BLP, виды запросов.
11. Описание take-grant модели, де-юре правила, условия передачи прав доступа для графа доступов, включающего только субъекты.
12. Механизмы ограничений в ролевой модели управления доступом.
13. Основные элементы модели ИПС, МБО и МБС, Корректность субъектов.
14. Описание расширенной take-grant модели, де-факто правила.
15. Политика low-watermark.
16. Скрытые (неявные) информационные потоки. Условия информационного потока в расширенной take-grant модели.
17. Мандатная ДП-модель и автоматные модели.
18. Политика, модель, правила и механизм управления доступом.
19. Модель целостности Биба.
20. Модель контроля доступа на основе атрибутов (ABAC).
21. IBAC и её реализации, LBAC и MLS, TBAC.
22. Граф доступов для tg-модели, модели BLP. Состояния данных моделей и переходы между ними.

Критерии оценивания:

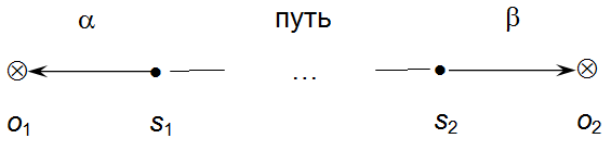
За основу берётся средняя оценка по итогам контрольных работ. Каждый правильный ответ на экзамене добавляет к ней 0.5 балла, каждый неправильный – отнимает 0.5. Зачёт за сделанный доклад прибавляют к оценке 0.5 балла. Отметка «зачтено» за

лабораторный проект прибавляет 1 балл, «условно зачтено» – 0.5. Итоговая оценка округляется в меньшую сторону.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Задачи

1. Пусть возможна передача прав доступа в одну сторону. Возможна ли она в противоположную сторону? (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1-2)



Ответ: да, в ответе необходимо продемонстрировать механизм передачи.

2. Нарисовать граф доступов, нарушающий ss-свойство. (ИОПК-8.3, ИОПК-11.1-3, ИПК-2.2)

Ответом является граф доступа, где субъект обладает доступом на чтение объекта большего уровня, чем субъект.

3. Нарисовать граф доступов, нарушающий *-свойство. (ИОПК-8.3, ИОПК-11.1-3, ИПК-2.2)

Ответом является граф доступа, где субъект обладает доступом на запись в объект меньшего уровня, чем субъект.

4. Привести пример системы контроля доступа на основе списков или матрицы доступа. (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

5. Привести пример системы контроля доступа на основе ролей. (ИОПК-11.1-3, ИПК-2.1-2)

6. Привести пример системы контроля доступа на основе решёток уровней конфиденциальности. (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

7. Привести пример системы контроля доступа на основе атрибутного контроля доступа. (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)

Ответ на вопросы 4-7 может быть дан в форме рисунка или текстового описания и должен содержать указанный механизм.

Теоретические вопросы.

1. Сущность, объект, субъект, контейнер (ИОПК-11.1, ИОПК-8.3, ИОПК-11.3, ИПК-2.1)
2. Права доступа и доступы (ИОПК-11.1, ИОПК-8.3, ИОПК-11.3, ИПК-2.1)
3. Дискреционная и мандатная политика (ИОПК-11.1, ИОПК-8.3, ИОПК-11.3, ИПК-2.1)
4. Модель контроля доступа как автомат, траектория функционирования КС (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1-2)
5. Описание take-grant модели (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1-2)
6. Матрица доступа (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)
7. Уровни конфиденциальности и тематические метки (ИОПК-8.3, ИОПК-11.1-2, ИПК-2.1)
8. Ролевой контроль доступа (ИОПК-11.1-3, ИПК-2.1-2)

9. Основные элементы модели BLP (ИОПК-8.3, ИОПК-11.1-3, ИПК-2.2)
10. Основные элементы модели ИПС (ИОПК-11.1-2, ИПК-2.1)

Теоретические вопросы для проверки остаточных знаний предполагают краткое определение данного понятия и демонстрацию раскрывающий его примера, т.е. примеры субъектов и объектов в реальных КС, граф доступов take-grant модели и пример его изменения под действием правил и т.д.

Информация о разработчиках

Твардовский Александр Сергеевич, канд. физ.-мат. наук, доцент кафедры компьютерной безопасности