Приложение 1

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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор института прикладной
математики и компьютерных наук
_____А. В. Замятин
« 16 » июня 2023 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Модели безопасности компьютерных систем

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

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

Томск – 2023

ОМ составил(и):
канд. физ.-мат. наук
старший преподаватель кафедры компьютерной безопасности А.С. Твардовский

Рецензент:
канд. тех. наук, доцент
заведующий кафедрой компьютерной безопасности С.А. Останин

Оценочные средства одобрены на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 08 июня 2023 г. № 02

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Оценочные средства (ОС) являются элементом оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатываются в соответствии с рабочей программой (РП).

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	ИОПК-8.3 Проводит анализ и формализацию поставленных задач, участвует в разработке математических моделей в области обеспечения безопасности компьютерных систем и сетей.	ОР-8.3.1. Знать: назначение и формальное описание классических моделей безопасности (ХРУ, Белла-ЛаПадулы, Take-Grant). ОР-8.3.2. Уметь: разрабатывать подходящую модель для обеспечения безопасности компьютерных систем и сетей. ОР-8.3.3. Владеть: математическим аппаратом классических моделей управления доступом.	Знает назначение и формальное описание классических моделей безопасности, умеет разрабатывать подходящую модель для обеспечения безопасности компьютерных систем и сетей; владеет математическим аппаратом классических моделей управления доступом.	Знает назначение и формальное описание классических моделей безопасности; имеет базовые представления о разработке модели для обеспечения безопасности компьютерных систем и сетей; знаком с математическим аппаратом классических моделей управления доступом.	Имеет базовое представление о классических моделях безопасности; слабо знаком с разработкой моделей для обеспечения безопасности компьютерных систем и сетей; посредственно знаком с математическим аппаратом классических моделей управления доступом.	Не знает назначение и формальное описание классических моделей безопасности.

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	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.	ОР-11.1.1. Знать: основные формальные модели дискреционного, мандатного, ролевого управления доступом. ОР-11.1.2. Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах. ОР-11.2.1. Владеть: аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах ОР-11.2.2. Владеть: классическими политиками управления доступом, аппаратом их анализа и разработки. ОР-11.3.1. Уметь: формулировать свойства безопасности в соответствии с требованиями заданной политики. ОР-11.3.2. Уметь: разрабатывать политики безопасности компьютерных систем с учетом требований по защите информации.	Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, основные виды политик управления доступом и информационными потоками в компьютерных системах; владеет аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах, классическими политиками управления доступом, аппаратом их	Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, основные виды политик управления доступом и информационными потоками в компьютерных системах; имеет базовые представления о формальном определении требований политики безопасности, построении и анализе политик управления доступом и информационными потоками в компьютерных системах, классических политиках управления доступом,	Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, основные виды политик управления доступом и информационными потоками в компьютерных системах; имеет базовые представления о классических политиках управления доступом, аппарате их анализа и разработки; знаком с разработкой политики безопасности компьютерных систем с учетом требований по защите информации.	Не знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, основные виды политик управления доступом и информационными потоками в компьютерных системах.

			анализа и разработки; умеет формулировать свойства безопасности в соответствии с требованиями заданной политики, разрабатывать политики безопасности компьютерных систем с учетом требований по защите информации.	аппаратах их анализа и разработки; способен разрабатывать политики безопасности компьютерных систем с учетом требований по защите информации.		
ПК-2. Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей.	ИПК-2.1 Разрабатывает математические модели, реализуемые в средствах защиты информации.	ОР-2.1.1. Знать: модели изолированной программной среды и безопасности информационных потоков. ОР-2.1.2. Владеть: математическим аппаратом для анализа безопасности систем управления доступом. ОР-2.2.1. Уметь: разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем. ОР-2.2.2. Уметь: разрабатывать механизмы управления доступом для современных компьютерных систем.	Знает модели изолированной программной среды и безопасности информационных потоков; владеет математическим аппаратом для анализа безопасности систем управления доступом; умеет разрабатывать	Знает модели изолированной программной среды и безопасности информационных потоков; имеет базовые представления об анализе безопасности систем управления доступом; умеет разрабатывать механизмы	Знает модели изолированной программной среды и безопасности информационных потоков; умеет разрабатывать механизмы управления доступом для некоторых компьютерных систем.	Не знает модели изолированной программной среды и безопасности информационных потоков; не умеет разрабатывать механизмы управления доступом для современных компьютерных систем.

			модели угроз и модели нарушителя безопасности компьютерных систем, механизмы управления доступом для современных компьютерных систем.	управления доступом для современных компьютерных систем.		

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Основные элементы и виды управления доступом	ОР-11.1.1-2., ОР-8.3.1-2., ОР-11.3.1-2, ОР-2.2.1.	Решение задач на практиках Устный зачёт с оценкой
2.	Ролевая модель	ОР-11.1.1., ОР-11.2.2., ОР-2.1.2., ОР-11.3.1-2., ОР-2.2.2.	Групповой проект Решение задач на практиках Устный зачёт с оценкой
3.	Take-Grant модель	ОР-8.3.1., ОР-11.1.2., ОР-11.2.1., ОР-8.3.3., ОР-2.1.2., ОР-2.2.2.	Групповой проект Решение задач на практиках Устный зачёт с оценкой
4.	Модель изолированной программной среды и основы ДП моделей	ОР-2.1-2.1., ОР-11.1.2., ОР-11.2.1.	Решение задач на практиках Устный зачёт с оценкой
5.	Модели Белла-ЛаПадулы и Биба	ОР-8.3.1., ОР-8.3.3., ОР-11.3.1-2, ОР-11.1.2., ОР-11.2.1., ОР-2.1.2., ОР-2.2.2.	Групповой проект Решение задач на практиках Устный зачёт с оценкой
6.	Разработка механизмов управления доступом для современных компьютерным систем	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2., ОР-2.2.2.	Тестирование Выступление с докладом Групповой проект Решение задач на практиках Устный зачёт с оценкой

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Групповой проект

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

Требования к реализации

1) Наличие нескольких (не менее трёх) субъектов (групп субъектов) с различными параметрами доступов (уровнями доступа, ролями), различными ACL или строками матрицы доступов …

2) Наличие нескольких (не менее трёх) объектов (групп объектов) с различными параметрами ограничения доступа субъектов (уровней конфиденциальности, различными ACL, столбцами матрицы доступов и др.)

3) Система аутентификации

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

Допускаются группы от одного до трёх человек

Доклад

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, UNIX ACL, Windows ACL.
12. SELinux
13. XACML и его реализации
14. Реализация политики безопасности в облачных хранилищах

15. Реализации контроля доступа в СУБД
16. AppArmor
17. Система контроля доступа на конкретном примере

Примеры вопросов из теста

Пусть доступ (s, o, r) обладает *-свойством в системе, этот доступ может не обладать simple security свойством Ответ: неверно
Выделите элементы модели Белла-ла-Падулы Выберите один или несколько ответов: a. Множество возможных множеств текущих информационных потоков b. Множество возможных множеств текущих доступов (да) c. Решётка уровней конфиденциальности (да) d. Множество возможных матриц доступов (да) e. Множество субъектов и объектов (да) f. Функции уровней доступа и конфиденциальности (да)
Укажите мосты tg-модели Выберите один или несколько ответов: a. (t->)(g->)(t<-)(t<-) (да) b. (t<-)(t<-) (да) c. (t->) (да) d. (t->)(g->)(t->) e. (t->)(t->)(t->)(g<-) (да) f. (t->)(t<-)
Дана теорема. Система S(Q, D, W, z_0) обладает … для любого начального состояния z_0, обладающего …, тогда и только тогда, когда для каждого действия (q, d, (b*, m*, f*), (b, m, f)) из W выполняются условия 1, 2. *Условие* 1. Каждый доступ (s, o, r) из b* \ b обладает … относительно f*. *Условие* 2. Если (s, o, r) из b и не обладает … относительно f*, то (s, o, r) не принадлежит b*. Что необходимо добавить на место …, чтобы получилась одна из теорем безопасности модели BLP Выберите один или несколько ответов: a. simple security свойство (да) b. **-свойство c. *-свойство (да) d. ds-свойство (да)
Дан граф доступа G = (S, O, E), где O = {s_1, s_2, s_3, s_4, s_5, s_6} S = {s_1, s_2, s_3, s_4, s_5}, E = {(s_1, s_2, g), (s_2, s_3, t), (s_3, s_6, t), (s_5, s_6, t), (s_4, s_6, g)}. Запишите количество островов tg-модели Ответ: 3

Задачи для практических занятий

1. Построить все возможные пути длины 2 в графе доступов TG модели, определить, по каким из них возможна передача прав

2. Спроектировать ролевую политику контроля доступом для вебинара. Задать механизмы ограничений.
3. Дана система $S = \{s_1, s_2\}$, $O = \{o_1, o_2\}$, $R = \{read, write\}$, $(L, \leq) = (Low, High)$
$$f_s(s_1) = f_o(o_1) = Low, f_s(s_2) = f_o(o_2) = High$$
   - Описать её множество состояний
   - Подсчитать количество состояний для следующих случаев:
     1. не требуется выполнение свойств безопасности
     2. выполняется simple security свойство (Какие запрещённые потоки могут быть реализованы в данном случае?)
     3. выполняется simple security свойство и * свойство (Остались ли запрещённые потоки с прежнего пункта?)
4. Найти в приложении для организации вебинара субъекты, объекты, доступы, информационные потоки

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Список билетов к зачёту с оценкой

Билет 1

Базовая терминология (сущность, объект, субъект, контейнер), доступы, информационные потоки по памяти и времени.

Свойства безопасности модели BLP (simple security-свойство, *-свойство, ds-свойство). Теоремы безопасности и их доказательства.

Билет 2

Три аксиомы компьютерной безопасности.

Замыкание расширенной take-grant модели.

Билет 3

Дискреционная и мандатная политики. Основные признаки, преимущества и недостатки.

ИПС: МБО и МБС, Базовая теорема ИПС, Ядро безопасности и создание гарантированно защищенной КС.

Билет 4

Особенности и принципы ролевой модели управления доступом, иерархия ролей и критерии безопасности.

Формальное определение и основные элементы базовой ДП модели, условия передачи прав доступа.

Билет 5

Условия передачи прав доступа для произвольного графа доступов в базовой модели take-grant (мосты и острова), условия похищения прав доступа.

Основные элементы модели BLP, виды запросов.

Билет 6

Описание take-grant модели, де-юре правила, условия передачи прав доступа для графа доступов, включающего только субъекты.

Механизмы ограничений в ролевой модели управления доступом.

Билет 7

Основные элементы модели ИПС, МБО и МБС, Корректность субъектов.

Описание расширенной take-grant модели, де-факто правила.

Билет 8

Политика low-watermark.

Скрытые (неявные) информационные потоки. Условия информационного потока в расширенной take-grant модели.

Билет 9

Мандатная ДП-модель и автоматные модели.

Политика, модель, правила и механизм управления доступом.

Билет 10

Модель целостности Биба.

Модель контроля доступа на основе атрибутов (ABAC).

Билет 11

IBAC и её реализации, LBAC и MLS, TBAC.

Граф доступов для tg-модели, модели BLP. Состояния данных моделей и переходы между ними.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Для допуска к устному зачёту с оценкой необходимо прохождение текущей аттестации, которая включает следующие пункты.

1. Выполнение группового проекта
2. Прохождение итогового теста в системе moodle. Тест считается пройденным, если обучающийся верно ответил на 70% вопросов или более. В случае неудачи – предоставляется дополнительная попытка.
3. Выступление с докладом

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного зачёта с оценкой по теоретическому материалу. К зачёту допускаются только студенты, успешно прошедшие текущие аттестации.

Каждый билет для устного зачёта состоит из двух теоретических вопросов по двум темам дисциплины.