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

Радиофизический факультет

УТВЕРЖДЕНО:
Декан
А. Г. Коротаев

Оценочные материалы по дисциплине

Анализ безопасности компьютерных систем

по направлению подготовки

03.04.03 Радиофизика

Направленность (профиль) подготовки:
Радиофизика, электроника и информационные системы

Форма обучения
Очная

Квалификация
Магистр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
Д.Я. Суханов

Председатель УМК
А.П. Коханенко

Томск – 2025

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен применять фундаментальные знания в области физики и радиофизики для решения научно-исследовательских задач, в том числе в сфере педагогической деятельности;.

ОПК-2 Способен определять сферу внедрения результатов прикладных научных исследований в области своей профессиональной деятельности;.

ОПК-3 Способен применять современные информационные технологии, использовать компьютерные сети и программные продукты для решения задач профессиональной деятельности..

ПК-1 Способен производить анализ состояния научно-технической проблемы, технического задания, формулировать цель и задачи научного исследования в области радиофизики и электроники.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Представляет современную научную картину мира, выявляет естественнонаучную сущность проблемы, формулирует задачи в области радиофизики и радиоэлектроники и определяет пути их решения

ИОПК 1.2 Организует проведение научного исследования и разработку в области радиофизики и радиоэлектроники

ИОПК 2.1 Представляет и аргументированно защищает полученные результаты профессиональной деятельности

ИОПК 2.2 Оценивает прикладные результаты профессиональной деятельности, предлагает возможные области их применения и целесообразный режим правовой охраны в качестве интеллектуальной собственности

ИОПК 3.1 Осуществляет поиск научно-технической информации с использованием информационных технологий

ИОПК 3.2 Предлагает новые идеи и подходы к решению научно-исследовательских и прикладных задач с использованием информационных систем и технологий

ИПК 1.1 Формулирует проблему и определяет предметную область исследования

ИПК 1.2 Проводит поиск и анализ научно-технической информации и патентной документации, отечественного и зарубежного опыта в выбранной области радиофизики и электроники

ИПК 1.3 Представляет информацию в систематизированном виде, формулирует цель исследования

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тест.

Тест (ИОПК 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, ИПК 1.1 – 1.3)

1. Что понимается под безопасностью информации
   а) состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность;
   б) состояние информации быть доступной только ограниченному кругу пользователей;
   в) способность совершать действия незаметно для других.
2. Что понимается под конфиденциальностью информации
   а) быть доступной только ограниченному кругу пользователей;
   б) способность сохранять свое содержание/структуру в процессе хранения/передачи;

в) способность совершать действия незаметно для других.

3. Что понимается под целостностью информации
   а) информация не изменяется при передаче и хранении;
   б) информация может изменяться при выполнении операций над ней;
   в) быть доступной только ограниченному кругу пользователей.
4. Укажите, что не является признаком защищенности КС
   а) разграничения доступа пользователей к объектам;
   б) идентификация пользователя;
   в) противодействие выводу из строя КС;
   г) доступность любой информации каждому пользователю.
5. Что понимается под политикой безопасности
   а) набор правил, на которых строится управление, защита и распределение информации в сети;
   б) набор матриц доступов;
   в) набор уровней допуска.
6. Укажите основные виды политики безопасности
   а) избирательная;
   б) полномочная;
   в) субъектная;
   г) объектная.
7. Какая модель не является моделью безопасности КС
   а) модель систем дискреционного разграничения доступа;
   б) модель систем мандатного разграничения доступа;
   в) модель безопасности информационных потоков;
   г) модель ролевого разграничения доступа;
   д) субъектно-ориентированная модель изолированной программной среды;
   е) реляционная модель.
8. Что не включает в себя политика безопасности КС
   а) множество субъектов;
   б) множество объектов;
   в) множество возможных операций над объектами;
   г) множество разрешенных операций для каждой пары субъект-объект;
   д) идентификация субъектов системы.
9. Укажите свойства дискреционного управления доступом
   а) все субъекты и объекты должны быть идентифицированы;
   б) права доступа субъекта к объекту определяются набором правил;
   в) каждый субъект имеет права доступа к любому объекту.
10. В чем заключается мандатная модель политики безопасности
   а) все субъекты и объекты должны быть идентифицированы;
   б) каждому объекту присвоен уровень допуска;
   в) каждому субъекту присвоен уровень доступа;
   г) каждый субъект имеет права доступа к любому объекту.

Ключи: 1 а), 2 а), 3 а), 4 г), 5 а), 6 а, б), 7 е), 8 д), 9 а, б), 10 а, б, в).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на половину вопросов.

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

Экзаменационный билет состоит из двух частей.

Первый вопрос в каждом билете сформулирован для проверки сформированности следующих компетенций/индикаторов компетенций: ОПК-1, ИОПК 1.1, ИОПК 1.2, ОПК-2, ИОПК 2.1, ИОПК 2.2.

Второй вопрос в каждом билете сформулирован для проверки сформированности следующих компетенций/индикаторов компетенций: ОПК-3, ИОПК 3.1, ИОПК 3.2, ПК-1, ИПК 1.1, ИПК 1.2, ИПК 1.3.

Перечень теоретических вопросов:

1. Компьютерная система.
2. Объекты в компьютерной системе.
3. Информационный поток между объектами.
4. Виды доступа к объектам в компьютерной системе.
5. Свойства безопасности информации.
6. Угрозы безопасности информации.
7. Дискреционная политика безопасности.
8. Мандатная политика безопасности.
9. Политика безопасности информационных потоков.
10. Политика ролевого разграничения доступа.
11. Политика изолированной программной среды.
12. Модель матрицы доступов Харрисона-Руззо-Ульмана.
13. Анализ безопасности систем Харрисона-Руззо-Ульмана.
14. Модель типизированной матрицы доступов.
15. Классическая модель Take-Grant.
16. Базовая ДП-модель.
17. Субъектно-ориентированная модель изолированной программной среды.
18. Классическая модель Белла-ЛаПадулы.
19. Базовая модель ролевого управления доступом.

Критерии оценивания:
Результаты зачета определяются оценками «зачтено», «незачтено».
Оценка «зачтено» выставляется, если даны правильные ответы на все вопросы.
Оценка «незачтено» выставляется, если один из вопросов билета не освещен.

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

Тест

1. Что понимается под конфиденциальностью информации
   а) быть доступной только ограниченному кругу пользователей;
   б) способность сохранять свое содержание/структуру в процессе хранения/передачи;
   в)способность совершать действия незаметно для других.
2. Что понимается под целостностью информации
   а) информация не изменяется при передаче и хранении;
   б) информация может изменяться при выполнении операций над ней;
   в) быть доступной только ограниченному кругу пользователей.
3. Основные свойства безопасности информации
   а) оперативность;
   б) конфиденциальность;
   в) целостность;
   г) доступность.
4. Что не является угрозой безопасности информации

а) угроза конфиденциальности;
б) угроза целостности;
в) угроза доступности;
г) угроза раскрытия параметров компьютерной системы;
д) изменение пароля пользователя.

5. Что не является видом доступа к объектам в компьютерной системе
а) чтение (read);
б) запись (*write*),
в) владение (own);
г) M – матрица доступов.

6. Что не является элементом модель матрицы доступов Харрисона-Руззо-Ульмана
а) O – множество объектов;
б) S – множество субъектов O;
в) R – множеств видов прав доступа субъектов на объекты;
г) M – матрица доступов, строки которой соответствуют субъектам, а столбцы соответствующим объектам. $M[s,o] \subseteq R$ – права доступа субъекта s на объект o;
д) граф доступов.

7. Что не является элементом классической модели Take-Grant
а) O – множество объектов;
б) S – множество субъектов O;
в) $R = \{r_1, r_2, r_m\} \cup \{t, g\}$ – множество видов прав доступа;
г) $G = (S, O, E)$ – конечный помеченный ориентированный без петель граф доступов, описывающий состояние системы;
д) матрица доступов.

8. Укажите элементы модели Белла-ЛаПадулы
а) O – множество объектов;
б) S – множество субъектов O;
в) L – уровень безопасности, принадлежащей множеству уровней безопасности
г) $F : S \cup O \rightarrow L$ – функции безопасности;
д) решетка уровней секретности;
е) матрица доступов.

Ключи: 1 а), 2 а), 3 б, в, г), 4 д), 5 г), 6 д), 7 д), 8 а, б, в, г, д).

Информация о разработчиках

Прокопенко Светлана Анатольевна, к.т.н., доцент, ТГУ, доцент