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
« 19 » мая 2022 г.

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

Защита информации на аппаратном уровне

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Томск – 2022

ОМ составил(и):
канд. техн. наук, доцент,
зав. кафедры компьютерной безопасности С.А. Останин

Рецензент:
канд. техн, доцент,
доцент кафедры компьютерной безопасности В.В. Андреева

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

Протокол от 12 мая 2022 г. № 4

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
ПК-2 – Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.	ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем. ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем. ИПК-2.1 Осуществляет проведение контрольных	ОР-2.3.1 Владеть: навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем; ОР-2.2.1 Уметь: разрабатывать требования к безопасному функционированию телекоммуникационных систем и оценивать их работоспособность и эффективность; ОР-2.1.1 Уметь: разрабатывать требования к программно-аппаратным реализациям криптографических алгоритмов и оценивать их	Обучающийся полностью владеет материалом. Обладание обучающимся навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем; умение разрабатывать требования к безопасному функционированию телекоммуникационны	В целом успешные, но содержащие отдельные пробелы в знании материала. Обладание обучающимся навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и	Фрагментарно, неполное без грубых ошибок знание материала. Обладание обучающимся навыками проведения контрольных проверок работоспособности.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки

	проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.	работоспособность и эффективность в рамках поставленной задачи.	х систем и программно-аппаратным реализациям криптографических алгоритмов и оценивать их работоспособность и эффективность в рамках поставленной задачи.	механизмов их реализации для разработки безопасных 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.	Тема 1	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
2.	Тема 2	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
3.	Тема 3	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
4.	Тема 4	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
5.	Тема 5	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
6.	Тема 6	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
7.	Тема 7	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
8.	Тема 8	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты
9.	Тема 9	ОР-2.3.1, ОР-2.2.1, ОР-2.1.1	тесты

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Примерный перечень вопросов для тестов:

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню С2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню А1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню С2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.
16. Назовите основные категории атак.
17. Какой тип доступа требуется для выполнения атак доступа к документам?
18. Почему атаки перехвата выполнить труднее, чем прослушивание?
19. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
20. Для какого типа атак эффективным инструментом является разрыв кабеля?
21. Против каких свойств информации направлена атака на отказ от обязательств?

22. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
23. Всегда ли атака модификации включает в себя атаку доступа?
24. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?
25. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?
26. К какому типу атак особенно уязвимы беспроводные сети?
27. Примером атаки какого рода является изменение заголовка электронной почты?
28. Что является целью атак на отказ в обслуживании?
29. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
30. Что является первым шагом при выполнении атаки модификации электронной информации?
31. Выделите два основных типа межсетевых экранов.
32. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
33. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
34. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
35. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
36. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
37. Что должен обеспечивать межсетевой экран для проверки состояния?
38. При каком условии межсетевой экран прикладного уровня может называться гибридным?
39. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
40. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Примерный перечень вопросов для зачета:

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню С2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню А1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню С2 "Оранжевой книги"?

10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.
16. Назовите основные категории атак.
17. Какой тип доступа требуется для выполнения атак доступа к документам?
18. Почему атаки перехвата выполнить труднее, чем прослушивание?
19. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
20. Для какого типа атак эффективным инструментом является разрыв кабеля?
21. Против каких свойств информации направлена атака на отказ от обязательств?
22. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
23. Всегда ли атака модификации включает в себя атаку доступа?
24. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?
25. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?
26. К какому типу атак особенно уязвимы беспроводные сети?
27. Примером атаки какого рода является изменение заголовка электронной почты?
28. Что является целью атак на отказ в обслуживании?
29. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
30. Что является первым шагом при выполнении атаки модификации электронной информации?
31. Выделите два основных типа межсетевых экранов.
32. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
33. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
34. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
35. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
36. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
37. Что должен обеспечивать межсетевой экран для проверки состояния?
38. При каком условии межсетевой экран прикладного уровня может называться гибридным?
39. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
40. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

В течение семестра необходимо выполнение всех обязательных тестов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме зачета с оценкой по теоретическому материалу.