Приложение 1

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
«16» июня 2023 г.

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

Информационная безопасность и работа с персональными данными

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Обработка данных, управление и исследование сложных систем

Томск – 2023

ОС составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности В.Н. Тренькаев

Рецензент:
канд. техн. 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 08.06.2023 № 02

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

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

ОС разрабатываются в соответствии с рабочей программой (РП) дисциплины.

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

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения**	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-1. Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	ИОПК-1.1. Анализирует проблемы в области прикладной математики, фундаментальной информатики и информационных технологий. ИОПК-1.2. Формулирует задачи исследования.	ОР-1.1.1 Обучающийся сможет проводить анализ проблем в области прикладной математики, фундаментальной информатики и информационных технологий. ОР-1.2.1 Обучающийся сможет формулировать задачи исследования в области прикладной математики, фундаментальной информатики и информационных технологий.	Демонстрация высокого уровня умений самостоятельного анализа проблем и формулировки задачи исследования в области прикладной математики, фундаментальной информатики и информационных технологий.	В целом успешные, но содержащие отдельные пробелы умения анализа проблем и при формулировке задачи исследования в области прикладной математики, фундаментальной информатики и информационных технологий.	Фрагментарное, неполное, без грубых ошибок, умение самостоятельного анализа проблем и формулировки задачи исследования в области прикладной математики, фундаментальной информатики и информационных технологий.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки при анализе проблем и формулировке задачи исследования в области прикладной математики, фундаментальной информатики и информационных технологий.

	ИОПК-1.3Решает актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	ОР-1.3.1 Обучающийся сможет решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	Демонстрация высокого уровня умений решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	В целом успешные, но содержащие отдельные пробелы умения решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	Фрагментарное, неполное, без грубых ошибок, умение решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	Не имеет четкого представления о способах решения актуальных проблем прикладной математики, фундаментальной информатики и информационных технологий.
ОПК-4. Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ИОПК-4.2. Учитывать основные требования информационной безопасности.	ОР-4.2.1 Обучающийся сможет учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.	Демонстрация высокого уровня умений учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.	В целом успешные, но содержащие отдельные пробелы в умении учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.	Фрагментарное, неполное, без грубых ошибок, умение учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки при анализе основных требований информационной безопасности при решении задач в области профессиональной деятельности.

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.	Общие понятия информационной безопасности	ОР-1.1.1, ОР-1.2.1, ОР-1.3.1, ОР-4.2.1	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
2.	Методы обеспечения информационной безопасности	ОР-1.1.1, ОР-1.2.1, ОР-1.3.1, ОР-4.2.1	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
3.	Средства обеспечения информационной безопасности	ОР-1.1.1, ОР-1.2.1, ОР-1.3.1, ОР-4.2.1	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
4.	Стандарты и нормативные документы информационной безопасности	ОР-1.1.1, ОР-1.2.1, ОР-1.3.1, ОР-4.2.1	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Типовые варианты заданий для лабораторных работ.

Тема: Общие понятия информационной безопасности. Цель: научить студентов владению основными понятиями информационной безопасности. Студент должен самостоятельно выполнить задание, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными понятиями информационной безопасности. Вариант задания: используя Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), изучить угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), характерные для выбранного студентом IT-объекта (облачные сервис, грид-система, BIOS, виртуальная среда, беспроводная сеть, ОС, web-приложение, хранилище больших данных, прикладное ПО и пр.), а также известные устраненные уязвимости для выбранного типа ПО (СУБД, АСУ ТП и т.п.).

Тема: Методы обеспечения информационной безопасности. Цель: научить студентов владению основными методами обеспечения информационной безопасности. Студент должен самостоятельно выполнить задания, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными методами обеспечения информационной безопасности. Вариант задания "Классические шифры замены и перестановки": зашифровать свое ФИО: 1) лозунговым шифром; 2) шифром Виженера; 3) шифром вертикальной перестановки; расшифровать произвольное слово из предложенного списка и зашифрованное шифром Виженера при известном ключе.
Задание "Современные симметричные шифры".

Тема: Средства обеспечения информационной безопасности. Цель: научить студентов владению основными средствами обеспечения информационной безопасности. Студент должен самостоятельно выполнить задания, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными средствами обеспечения информационной безопасности. Вариант задания "Встроенные средства защиты ОС Windows": написать краткий обзор методов и средств обеспечения информационной безопасности ОС Windows 10 на основе различных источников информации: официальный сайт компании Microsoft, учебные интернет-курсы Национального Открытого Университета «ИНТУИТ» и пр, используя консоль управления mmc (Microsoft Management Console), выполнить различные задания преподавателя, связанные с управлением доступом к данным, аудитом системы, работой с диспетчером сертификатов, созданием шаблона безопасности.

Тема: Стандарты и нормативные документы информационной безопасности. Цель: научить студентов владению основными стандартами и нормативными документами информационной безопасности. Студент должен самостоятельно выполнить задание, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными основными стандартами и нормативными документами информационной безопасности. Вариант задания "Руководящие документы Гостехкомиссии России": на сайте ФСТЭК России (Федеральная служба по техническому и экспортному контролю) http://fstec.ru/ найти Государственный реестр сертифицированных средств защиты информации, в данном реестре выбрать средство защиты, которое имеет сертификат на соответствие одному или нескольким руководящим документам либо по уровню контроля отсутствия НДВ (недекларированных возможностей), либо по классу защищенности СВТ (средств вычислительной техники), либо по классу защищенности МЭ (межсетевых экранов), либо по классу защищенности АС (автоматизированных систем), изучить соответствующий(ие) руководящий(ие) документ(ы), описать требования, которые предъявляются к выбранному средству защиты с точки зрения соответствия заданному классу защищенности, и выложить в систему Moodle.

Примерный перечень вопросов текущего контроля:

1. Дать определение одного их следующих понятий: шифр, секретный ключ, шифрование данных, симметричный шифр, асимметричный шифр, открытый ключ, закрытый ключ, хэш-функция (ключевая и безключевая), электронная цифровая подпись, аутентификация, протоколирование, активный аудит, управление доступом, матрица доступа, межсетевое экранирование, туннелирование, компьютерный вирус, политики безопасности, VPN-шлюз (шлюз безопасности).
2. Перечислить известные криптографические алгоритмы, используемые на практике (симметричные шифры, асимметричные шифры, хэш-функции, цифровые подписи).
3. Изложить основные свойства электронной цифровой подписи (хэш-функции).

4. Поставить задачу активного аудита/управление доступом/межсетевого экранирования.
5. Изложить функции межсетевого экрана (фильтрация и посредничество) и представить межсетевой экран моделью последовательности фильтров.
6. Перечислить параметры, по которым можно производить анализ информационного потока, существующие методы построения VPN-шлюзов, типичные проблемы, решаемые при анализе защищенности.
7. Объяснить функции системы обнаружения атак (СОА), перечислить виды сенсоров (агентов) СОА, охарактеризовать методы анализа СОА
8. Привести примеры классов (показателей) защищенности в соответствии с Руководящими документами Гостехкомиссии России.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Примерный перечень вопросов к зачету с оценкой:

1. Изложить основные понятия информационной безопасности (ИБ).
2. Классифицировать атаки на компьютерные сети.
3. Перечислить атаки на коммуникационные протоколы.
4. Описать законодательные методы обеспечения ИБ.
5. Описать административно-организационные методы обеспечения ИБ.
6. Сравнить симметричные и асимметричные шифры.
7. Предоставить схему гибридной (комбинированной) криптосистемы.
8. Предоставить схему электронной цифровой подписи.
9. Изложить метод обеспечения целостности сообщения.
10. Изложить основные свойства электронной цифровой подписи.
11. Охарактеризовать парольный метод аутентификации.
12. Охарактеризовать аппаратную аутентификацию.
13. Охарактеризовать биометрическую аутентификацию.
14. Охарактеризовать аутентификацию на основе цифровых сертификатов.
15. Охарактеризовать аутентификацию на базе протокола «запрос-ответ».
16. Перечислить цели и задачи протоколирования и аудита.
17. Охарактеризовать статистический метод обнаружения атак.
18. Охарактеризовать сигнатурный метод обнаружения атак.
19. Охарактеризовать дискреционное управление доступом.
20. Охарактеризовать мандатное управления доступом.
21. Охарактеризовать ролевое управление доступом.
22. Перечислить функции, которые может выполнять межсетевой экран.
23. Классифицировать компьютерные вирусы и вредоносные программы.
24. Изложить способы распространения и обнаружения вредоносных программ.
25. Изложить типовое содержание политики безопасности предприятия.
26. Охарактеризовать технологию построения виртуальных частных сетей.
27. Охарактеризовать технологию анализа защищенности сети.
28. Охарактеризовать технологию обнаружение атак на компьютерные сети.
29. Классифицировать системы обнаружения атак.

30. Охарактеризовать стандартные средства системы безопасности операционных систем.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Выполнение лабораторной работы оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до зачета с оценкой является выполнение 80% лабораторных работ, с оценкой за каждую не менее 80 баллов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Критерии выставления оценок (для зачета с оценкой):

1. Отлично - Магистр показал творческое отношение к обучению, в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях
2. Хорошо - Магистр овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.
3. Удовлетворительно - Магистр имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.
4. Неудовлетворительно - Магистр имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.