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_____ 20_23_ г.

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

Основы информационной безопасности

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

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

Томск – 2023

ОМ составил(и):
ФОС составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности  В.Н. Тренькаев

Рецензент:
канд. техн. наук,
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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности; ИОПК-1.2 Понимает значение информации, информационных технологий и информационной безопасности в развитии современного общества; ИОПК-1.3 Выявляет влияние информации, информационных технологий и информационной	ОР-1.1.1. **Знать**: механизмы и элементы государственной системы обеспечения информационной безопасности.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

	безопасности на объективные потребности личности, общества и государства.					
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности.	ОР-8.1.1 **Владеть**: понятийным аппаратом информационной безопасности. ОР-8.1.2 **Уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.	Отлично сформированное умение классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Демонстрация высокого уровня владения понятийным аппаратом информационной безопасности	Хорошее умение классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. В целом высокий, но содержащий отдельные пробелы, уровень владения понятийным аппаратом информационной безопасности	Удовлетворительное умение классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. . Фрагментарное, неполное владение без грубых ошибок понятийным аппаратом информационной безопасности	Неудовлетворительное умение классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Не имеет представления об понятийном аппарате информационной безопасности.
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей	ОР-9.1.1. **Знать**: угрозы информационной безопасности и меры противодействия им. ОР-9.1.2 **Знать**: основные средства и способы обеспечения информационной безопасности.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	профессиональной деятельности.					
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.	ОР-10.1.1 **Уметь**: формулировать предложения по применению криптографических средств защиты информации	Отлично сформированное умение формулировать предложения по применению криптографических средств защиты информации	Хорошее умение формулировать предложения по применению криптографических средств защиты информации	Удовлетворительное умение формулировать предложения по применению криптографических средств защиты информации .	Неудовлетворительное умение формулировать предложения по применению криптографических средств защиты информации

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.	Информация как объект защиты.	ОР-8.1.2 Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.	задания, вопросы, конспект самоподготовки, собеседование
2.	Понятийный аппарат информационной безопасности.	ОР-8.1.1 Владеть: понятийным аппаратом информационной безопасности.	задания, вопросы, конспект самоподготовки, собеседование.
3	Государственная политика информационной безопасности	ОР-1.1.1. Знать: механизмы и элементы государственной системы обеспечения информационной безопасности.	задания, вопросы, конспект самоподготовки, собеседование
4	Угрозы безопасности информации.	ОР-9.1.1. Знать: угрозы информационной безопасности и меры противодействия им.	задания, вопросы, конспект самоподготовки, собеседование.
5	Меры противодействия угрозам безопасности.	ОР-9.1.1. Знать: угрозы информационной безопасности и меры противодействия им.	задания, вопросы, конспект самоподготовки, собеседование
6	Криптографические методы защиты информации.	ОР-10.1.1 Уметь: формулировать предложения по применению криптографических средств защиты информации	задания, вопросы, конспект самоподготовки, собеседование.
7	Основные механизмы защиты от несанкционированного доступа	ОР-9.1.2 Знать: основные средства и способы обеспечения информационной безопасности.	задания, вопросы, конспект самоподготовки, собеседование
8	Информационная безопасность компьютерных сетей.	ОР-9.1.2 Знать: основные средства и способы обеспечения информационной безопасности.	задания, вопросы, конспект самоподготовки, собеседование.

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Тема “Понятийный аппарат информационной безопасности”. Задание. Используя Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), требуется детально изучить три угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), присущих некоторому одному выбранному студентом объекту (облачная система, грид-система, BIOS, виртуальная машина, беспроводная сеть, web-приложение, хранилище больших данных и т.п.), а также три устраненные уязвимости для некоторого одного выбранного студентом ПО (СУБД MySQL, браузер Google Chrome и т.п.). Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение основными понятиями информационной безопасности. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы: 1) список определений терминов: угроза, уязвимость, конфиденциальность, целостность, доступность; 2) список изученных угроз и уязвимостей.

Тема “Информационная безопасность компьютерных сетей”. Задание. Требуется выбрать какое-либо программное средство защиты информации (СЗИ) от какого-либо производителя, изучить предназначение системы/средства/инструмента: какие задачи решаются и какие методы/подходы/алгоритмы используются для решения данных задач, архитектуру (схему работы), функциональные возможности и характеристики средства. Излученный материал излагается в виде краткого реферата с указанием источников информации. После чего надо скачать, установить пробную версию изученного СЗИ, и настроить, активизируя базовые возможности продукта. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы в виде реферата и скриншотов (снимков экрана) с настройками СЗИ. Примеры СЗИ: КриптоПро CSP – криптопровайдер, Secret Net Studio - защита конечных точек, Kaspersky Small Office Security - защита для малого бизнеса.

Тема “Криптографические методы защиты информации”. Задание “Шифры замены и перестановки”. Требуется 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. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы.

Тема “Основные механизмы защиты от несанкционированного доступа”. Задание “Руководящие документы”. Используя сайт ФСТЭК России (Федеральная служба по техническому и экспортному контролю) http://fstec.ru/, выбрать СЗИ в Государственном реестре сертифицированных средств защиты информации, 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 классу защищенности выбранного СЗИ. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Примерный перечень вопросов к зачету:

1. Уровни представления информации.
2. Свойства защищаемой информации.
3. Виды тайн (государственная, служебная, профессиональная,…).
4. Термины, относящиеся к видам защиты информации.
5. Термины, относящиеся к способам защиты информации.
6. Термины, относящиеся к замыслу защиты информации.
7. Термины, относящиеся к объекту защиты информации.
8. Термины, относящиеся к угрозам безопасности информации.
9. Термины, относящиеся к технике защиты информации.
10. Национальная безопасность РФ.
11. Доктрина информационной безопасности РФ.
12. Законодательная основа обеспечения информационной безопасности.
13. Нормативная основа обеспечения информационной безопасности.
14. Безопасность критической информационной инфраструктуры РФ.
15. Государственная система обеспечения информационной безопасности.
16. Несанкционированные операции с информацией.
17. Источники и классификация угроз.
18. Перечень типовых непреднамеренных искусственных угроз.
19. Перечень типовых преднамеренных искусственных угроз.
20. Классификация способов несанкционированного доступа.
21. Типовые атаки на коммуникационные протоколы.
22. Законодательные меры противодействия угрозам безопасности.
23. Организационные меры противодействия угрозам безопасности.
24. Физические и технические меры противодействия угрозам безопасности.
25. Аутентификация. Невозможность отказа от авторства.
26. Имитозащита. Цифровая подпись.
27. Симметричный / асимметричный шифр.
28. Криптографическая стойкость шифра.
29. Метод криптографического анализа.
30. Криптографический протокол.
31. Криптографическая хеш-функция.
32. Классификация криптопротоколов.
33. Свойства цифровой подписи.
34. Криптографические протоколы аутентификации сообщений.

35. Криптографические протоколы идентификации.
36. Объект, субъект, доступ к информации, правила разграничения доступа.
37. Идентификация, аутентификация, авторизация.
38. Протоколирование и аудит (активный аудит).
39. Статистический метод обнаружения атак.
40. Сигнатурный метод обнаружения атак.
41. Дискреционное управление доступом.
42. Мандатное управление доступом.
43. Ролевое управление доступом.
44. Защита информации при хранении и передаче.
45. Защита от вредоносных программ.
46. Виды компьютерных вирусов и вредоносных программ.
47. Защита межсетевого взаимодействия.
48. Предотвращение утечек информации.
49. Аудит безопасности.
50. Угрозы корпоративной сети. Защита периметра сети.
51. Основные механизмы защиты корпоративной сети.
52. Средства защиты информации: межсетевые экраны.
53. Средства защиты информации: виртуальные частные сети.
54. Средства защиты информации: системы анализа защищенности.
55. Средства защиты информации: системы обнаружения атак.
56. Системы предотвращения утечки конфиденциальной информации.
57. Политика информационной безопасности организации.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Выполнение заданий оценивается по бинарной системе (зачет/незачет): зачет - студент в целом удовлетворительно разбирается в задаче, хорошо знает материал, отвечает на вопросы с замечаниями или с негрубыми ошибками; незачет - студент слабо разбирается в задаче, плохо знает материал, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя. Допуском до зачета является выполнение 80% заданий.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Зачет по дисциплине – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства тестовых/контрольных заданий.

Незачет по дисциплине – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении тестовых/контрольных заданий.