

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
А.В. Замятин
« 08 » _____ 2021 г.



Фонд оценочных средств по дисциплине

Основы информационной безопасности

по направлению подготовки

02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность (профиль) подготовки :

DevOps-инженерия в администрировании инфраструктуры ИТ-разработки

Томск–2021

ОС составил(и):
канд. техн. наук,
доцент кафедры компьютерной безопасности



В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности



С.А.Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии
института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

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	
			Зачтено	Не зачтено
ОПК-3.Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения	ИОПК-3.1.Обладает необходимыми знаниями в области информационных технологий и программных средств	ОР-3.1.1. Знает угрозы информационной безопасности и меры противодействия им. ОР-3.1.2. Владеет понятийным аппаратом информационной безопасности.	Демонстрация высокого уровня владения понятийным аппаратом информационной безопасности и знаний угроз информационной безопасности и мер противодействия им. Владеет понятийным аппаратом информационной безопасности	Не имеет четкого представления об угрозах информационной безопасности и мер противодействия им, а также допускает грубые ошибки при использовании понятийного аппарата информационной безопасности. Не владеет понятийным аппаратом информационной безопасности

	<p>ИОПК-3.2. Применяет знания, полученные в области информационных технологий и программных средств, при решении задач профессиональной деятельности.</p>	<p>ОР-3.2.1. Знает основные средства и способы обеспечения информационной безопасности.</p> <p>ОР-3.2.2. Умеет корректно использовать криптографические системы обеспечения безопасности информации.</p> <p>ОР-3.2.3. Знает механизмы и элементы государственной системы обеспечения информационной безопасности.</p>	<p>Демонстрация высокого уровня знаний основных средств и способов обеспечения информационной безопасности, механизмов и элементов государственной системы обеспечения информационной безопасности; умеет корректно использовать криптографические системы обеспечения безопасности информации, знает механизмы и элементы государственной системы обеспечения информационной безопасности.</p>	<p>Не имеет четкого представления об основных средствах и способах обеспечения информационной безопасности, механизмах и элементах государственной системы обеспечения информационной безопасности, допускает грубые ошибки при применении криптографических систем обеспечения безопасности информации, не умеет корректно использовать криптографические системы обеспечения безопасности информации, знает механизмы и элементы государственной системы обеспечения информационной безопасности.</p>
<p>ПК-2. Способен проектировать базы данных, разрабатывать компоненты программных систем, обеспечивающих работу с базами данных, с помощью современных инструментальных средств и технологий</p>	<p>ИПК-2.3. Использует средства СУБД для выявления проблем производительности при выполнении и повышением пропускной способности базы данных</p>	<p>ОР-2.3.1 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.</p>	<p>Демонстрация высокого уровня умений при проведении классификации защищаемой информации по видам тайны и степеням конфиденциальности.</p>	<p>Не имеет четкого представления о видах тайны и степенях конфиденциальности информации. Не умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.</p>

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-3.1.2, ОР-2.3.1	задания, вопросы, конспект самоподготовки, собеседование
2.	Понятийный аппарат информационной безопасности.	ОР-3.1.1, ОР-3.1.2, ОР-2.3.1	задания, вопросы, конспект самоподготовки, собеседование.
3	Государственная политика информационной безопасности	ОР-3.2.3	задания, вопросы, конспект самоподготовки, собеседование
4	Угрозы безопасности информации.	ОР-3.1.1, ОР-3.1.2	задания, вопросы, конспект самоподготовки, собеседование.
5	Меры противодействия угрозам безопасности.	ОР-3.1.1, ОР-3.1.2	задания, вопросы, конспект самоподготовки, собеседование
6	Криптографические методы защиты информации.	ОР-3.2.2	задания, вопросы, конспект самоподготовки, собеседование.
7	Основные механизмы защиты от несанкционированного доступа	ОР-3.1.1, ОР-3.2.1	задания, вопросы, конспект самоподготовки, собеседование
8	Информационная безопасность компьютерных сетей.	ОР-3.1.1, ОР-3.2.1 ОР-3.2.3,	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 (в зависимости от вопроса требуется изложить или объяснить или поставить задачу или перечислить или описать или дать определение или классифицировать или охарактеризовать или сравнить):

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 межсетевое взаимодействие.
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 заданий.

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