Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра экономической информатики

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Образовательная программа: 09.04.03 Прикладная информатика, магистерская программа: Информационные технологии в моделировании и организации бизнес-процессов

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Информационная безопасность приведена в Таблице.

Таблица – Структура фонда оценочных средств (раздел 1)

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК.6 способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	з1. знать правовые основы информационной безопасности и принципы защиты	Защита персональных данных, ФЗ-152 Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций	РГЗ: Раздел Введение: Описание предприятия: основной бизнес-процесс, обеспечивающие бизнес-процессы и другие бизнес - процессы. Описание производственного процесса. Раздел 1: Выявление информационных потоков, средств их поддержки. Классификация результатов инвентаризации данных: Выявление информационных потоков, средств их поддержки в обязательном порядке требующих защиты.	Зачет, вопросы: Характеристика каналов утечки информации на объекте. Основные принципы создания систем ИБ и цели их реализации. Общая технология проведения инвентаризации информационной системы для анализа состояния информационной информации. Классификация категорий объектов информационной системы по результатам инвентаризации: уровни доступности, целостности, конфиденциальности.
ОПК.6	у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Методы защиты информации. Средства защиты и их классификация.	РГЗ: Раздел 2: От чего защищать ? Получение навыков выявления элементов информационного взаимодействия по результатам ДЦК – классификации; Получение навыков инвентаризации вредоносных воздействий и оценки степени их влияния; Отображение результатов оценки степени вредоносного воздействия в виде 2-х мерной матрицы. Лабораторная работа : Перечень вредоносных воздействий, наблюдаемых, предполагаемых и потенциально возможных	Зачет, вопросы: Технология обнаружения и идентификации вирусов на компьютере. Типовая технология установления полномочий пользователя. Классификация и характеристика локальных атак. Классификация и характеристика удаленных атак. Методика оценки рисков при создании системы ИБ.

ПК.5/НИ способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	з2. знать основные принципы разработки систем защиты в информационных системах	Инвентаризация информационных систем. Инвентаризация средств защиты, классификация защитных функций Технология защиты информации. Термины и определения.	РГЗ: Раздел 2: Как защищать ? Провести инвентаризацию имеющихся средств защиты. Заполнить таблицу оценки эффективности. Лабораторная работа : Перечень средств защиты, наблюдаемых, предполагаемых и потенциально возможных. Классификация средств защиты.	Зачет, вопросы : Характеристика, область применения и технология применения организационных средств защиты. Характеристика, область применения и технология применения законодательных средств защиты.
ПК.5/НИ	з3. знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	Выявление вредоносных воздействий на информационную систему Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Классификация данных по доступности, целостности, конфиденциальности Организационно-правовое обеспечение защиты информации.	РГЗ: Раздел 2: От чего защищать ? Выявление наиболее атакуемых информационных элементов, наиболее активных ВВ Отображение результатов оценки степени вредоносного воздействия в виде 2-х мерной матрицы. Лабораторная работа : Перечень вредоносных воздействий, анализ активности угроз, выявление уязвимостей	Зачет, вопросы: Классификация вредоносных программ. Технология обнаружения и идентификации вирусов на компьютере. Типовая технология установления полномочий пользователя. Классификация и характеристика локальных атак. Классификация и характеристика удаленных атак. Методика оценки рисков при создании системы ИБ.
ОПК.6 способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	з1. знать правовые основы информационной безопасности и принципы защиты	Защита персональных данных, ФЗ-152 Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций	РГЗ: Раздел 3: Как защищать ? Заполнить таблицу оценки эффективности работы средств защиты. Выявить незадействованные, слабо функционирующие и имеющие не использованный потенциал средства защиты. Лабораторная работа : Перечень средств защиты, наблюдаемых, предполагаемых и потенциально возможных. Классификация средств защиты	Зачет, вопросы: Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография. Электронная цифровая подпись, технология и проблемы применения. Технология защиты информации при передаче по каналам связи.
ОПК.6	у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Методы защиты информации. Средства защиты и их классификация.	РГЗ: Раздел 4: Повышение уровня защиты. По заполненной таблице оценки эффективности работы средств защиты выявить не использованный потенциал средств защиты. Лабораторная работа : Выявление наименее защищенных	Зачет, вопросы: Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография. Электронная цифровая подпись, технология и проблемы применения. Технология защиты информации при передаче по каналам связи.

			элементов, модификация используемых средств защиты	
ПК.5/НИ способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	з2. знать основные принципы разработки систем защиты в информационных системах	Инвентаризация информационных систем. Инвентаризация средств защиты, классификация защитных функций Технология защиты информации. Термины и определения.	РГЗ: Раздел 4: Повышение уровня защиты. По заполненной таблице оценки эффективности работы средств защиты выявить не использованный потенциал средств защиты. Рекомендации по их модификации Лабораторная работа : Выявление наименее защищенных элементов, модификация перечня средств защиты за счет новых регламента-циионных	Зачет, вопросы: Характеристика, область применения и технология применения аппаратных средств защиты.Характеристика, область применения и технология применения технических средств защиты.Характеристика, область и технология применения методов регламентации.Характеристика, область и технология применения программных средств защиты.Типовая технология установления подлинности пользователя.Технология установления подлинности пользователя методом паролей.Классификация методов и технология установления подлинности пользователя с использованием биометрических параметров человека. Технология антивирусной защиты

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности компетенций ОПК.6, ПК.5/НИ.
Экзамен проводится по тестам. Тестовое задание во время зачета формируется по следующему правилу: проверочные вопросы открытого и закрытого типа предлагаются в случайном порядке(список вопросов приведен ниже). Для закрытых вопросов перечень вариантов ответов предлагается тоже в случайном порядке. В заключении зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 3 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.6, ПК.5/НИ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно,

большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.