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

Кафедра теоретической и прикладной информатики

“УТВЕРЖДАЮ”
ДЕКАН ФПМИ
д.т.н., доцент В.С. Тимофеев
“___”_____ _____ г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## УЧЕБНОЙ ДИСЦИПЛИНЫ

**Программные средства защиты информации**

Образовательная программа: 02.04.03 Математическое обеспечение и администрирование информационных систем, магистерская программа: Математическое и программное обеспечение информационных технологий

Новосибирск 2015

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

Обобщенная структура фонда оценочных средств по дисциплине Программные средства защиты информации приведена в Таблице.

Таблица

| **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.10 владение навыками использования основных моделей информационных технологий и способов их применения для решения задач в предметных областях | у7. Уметь определять комплекс превентивных мер по защите конфиденциальных данных | Ассиметричное шифрование Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Симметричное шифрование | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br>Экзамен: вопросы 85-95<br>Экзамен: вопросы 96-106<br>Экзамен: задача 12<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11 |
| ОПК.11 владение навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования | у1. Уметь формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации | Ассиметричное шифрование Введение в биометрию Введение в теорию чисел Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Основные понятия криптологии | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br>Экзамен: вопросы 85-95<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 107-115<br>Экзамен: задачи 2-10<br>Экзамен: вопросы 1-15<br>Экзамен: задачи 2-10 |
| ОПК.4 владение теоретическими основами информатики как науки; знание проблем современной информатики, ее категории и связи с другими научными дисциплинами, понимание основных этапов и тенденции развития программирования, математического обеспечения и информационных, технологий | з1. Знать встроенные средства защиты информации | Абсолютно стойкий шифр. Применение режима однократного гаммирования. Моделирование работы n-разрядного скремблера Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES и российский стандарт шифрования ГОСТ 28147-89) Ассиметричное шифрование Блочные составные шифры и анализ методики многократного использования ключа и материала исходного блока информации (Сеть Фейстеля) Введение в биометрию Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Основные понятия криптологии Режимы работы блочных шифров.Схемы кратного шифрования Симметричное шифрование Электронная цифровая | | Экзамен: вопросы 85-95<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 96-106<br>Экзамен: задача 12<br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11<br>Экзамен: вопросы 1-15<br>Экзамен: вопросы 107-115 |

| | | | | |
|---|---|---|---|---|
| | | подпись | | |
| ОПК.4 | з5. Знать основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак | Ассиметричное шифрование Введение в биометрию Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Симметричное шифрование | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br><br>Экзамен: вопросы 16-23<br><br>Экзамен: вопросы 85-95<br><br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11 |
| ПК.1/НИ владение навыками применения математических основ информатики при разработке и исследовании нового программного обеспечения | у1. Уметь реализовывать алгоритмы шифрования | Абсолютно стойкий шифр. Применение режима однократного гаммирования. Моделирование работы n-разрядного скремблера Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES и российский стандарт шифрования ГОСТ 28147-89) Ассиметричное шифрование Блочные составные шифры и анализ методики многократного использования ключа и материала исходного блока информации (Сеть Фейстеля) Введение в биометрию Введение в теорию чисел Идентификация и аутентификация Комбинированные криптоалгоритмы (RSA и DES/ RSA и ГОСТ) Криптоалгоритмы с открытыми ключами. Генерация простого большого числа.Построение первообразного корня по модулю n. Обмен ключами по схеме Диффи-Хеллмана Режимы работы блочных шифров.Схемы кратного шифрования Симметричное шифрование Электронная цифровая подпись | | Экзамен: вопросы 85-95<br><br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11<br><br>Экзамен: вопросы 107-115<br><br>Экзамен: задачи 2-10 |

**2. Методика оценки этапов формирования компетенций в рамках дисциплины.**

Промежуточная аттестация по дисциплине проводится в 3 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.10, ОПК.11, ОПК.4, ПК.1/НИ.

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

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.10, ОПК.11, ОПК.4, ПК.1/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.