Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Организационное и правовое обеспечение информационной безопасности

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.2 Учитывает основные требования информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– ведение конспекта самоподготовки
– выполнение заданий самостоятельной работы;
– устный опрос на занятиях;
– коллоквиум;

Задания самостоятельной работы (ИОПК-4.2, ИПК-2.2, ИПК-2.3):

Задание 1.

Найти и выбрать сертифицированное средство защиты информации (СЗИ), соответствующее заданным параметрам. Описать характеристики выбранного СЗИ, соответствующие определенным нормативными документами ФСБ и ФСТЭК России требованиям.

Задание 2.

Описать возможные технические каналы утечки информации для заданного объекта информатизации и способы их нейтрализации.

Задание 3.

Определить уровень защищенности и актуальные угрозы информационной безопасности для заданной информационной системы персональных данных. Определить перечень мер и средств защиты информации, необходимых для нейтрализации выявленных угроз.

Темы опросов на занятиях (ИОПК-4.2, ИПК-2.1, ИПК-2.2, ИПК-2.3):

1. Система обеспечения информационной безопасности Российской Федерации. Регулирование процесса обеспечения информационной безопасности Российской Федерации.
2. Лицензирование в области информационной безопасности. Сертификация средств защиты информации.
3. Аккредитация. Аттестация объектов информатизации.
4. Принципы реализации технических каналов утечки информации.
5. Этапы построения системы защиты информации в организации.
6. Этапы определения уровня защищенности информационных систем персональных данных и актуальных угроз безопасности персональных данных.

Вопросы для коллоквиума (ИОПК-4.2, ИПК-2.1, ИПК-2.2, ИПК-2.3):

1. Организационные и правовые меры по защите информации. Государственные органы Российской Федерации в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности.
5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.

Элементы учебной деятельности	Максимальный балл с начала семестра
Конспект самоподготовки	5
Опрос на занятиях	15
Домашнее задание	20
Коллоквиум	20

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет проводится в письменном виде по билетам. Билет содержит два теоретических вопроса, проверяющих ИОПК-4.2, ИПК-2.3. Продолжительность зачета 1 час.

Вопросы к зачету:

1. Организационные и правовые меры по защите информации. Государственные органы РФ в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности, нормативно-правовые акты.

5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.
8. Технические каналы утечки акустической информации.
9. Технические каналы утечки информации, обрабатываемой с использованием основных технических средств и систем.
10. Этапы построения системы защиты информации в организации.
11. Модель угроз информационной безопасности. Основные положения.
12. Модель нарушителя информационной безопасности. Основные положения.
13. Законодательство в области защиты персональных данных. Этапы определения уровня защищенности информационных систем персональных данных.
14. Модель угроз информационной системы персональных данных. Оценка актуальности угроз.

Максимальный балл за ответы на вопросы билета – 40. Студент должен дать развернутый ответ на каждый теоретический вопрос.

Пересчет баллов в оценки промежуточной успеваемости

Баллы на дату аттестации	Оценка
≥ 60% от максимальной суммы баллов	зачтено
<60% от максимальной суммы баллов	не зачтено

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИОПК-4.2):

1. Какие организационные и правовые меры по защите информации вы знаете.
2. Назовите основные нормативно-правовые акты в области информационной безопасности.
3. Назовите виды конфиденциальной информации.
4. Технические каналы утечки информации, обрабатываемой с использованием основных технических средств и систем.
5. Модель угроз информационной безопасности. Основные положения.
6. Законодательство в области защиты персональных данных. Этапы определения уровня защищенности информационных систем персональных данных.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент кафедры компьютерной безопасности.