

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 / специальности

10.05.01 Компьютерная безопасность

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

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Треньяев

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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-5.1 Обладает необходимыми знаниями нормативно-правовой базы, регламентирующей деятельность по защите информации

ИОПК-5.2 Определяет подлежащие применению нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

ИОПК-6.1 Понимает нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ИОПК-6.2 Предпринимает необходимые действия по организации защиты информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- ведение конспекта самоподготовки
- задания для самостоятельного выполнения;
- опрос на занятиях;
- коллоквиум.

Типовые задания для самостоятельного выполнения (ИОПК-5.1, ИОПК-5.2, ИОПК-6.1, ИОПК-6.2)

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-5.1, ИОПК-6.1):

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-5.1, ИОПК-5.2, ИОПК-6.1, ИОПК-6.2):

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-5.1, ИОПК-5.2, ИОПК-6.1. 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
$\geq 60\%$ от максимальной суммы баллов	зачтено
$<60\%$ от максимальной суммы баллов	не зачтено

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

Теоретические вопросы (ИОПК-5.1, ИОПК-5.2, ИОПК-6.1):

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.

Теоретические вопросы для проверки остаточных знаний предполагают краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

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