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

Защита информации от утечки по техническим каналам

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. Тренькаев

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 анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.1 Понимает основные физические законы и модели, выявляет естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности

ИОПК-4.2 Применяет соответствующий физико-математический аппарат для формализации, анализа и выработки решения проблем, возникающих в ходе профессиональной деятельности

ИОПК-4.3 Анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники

ИОПК-9.3 Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

– реферат;

– лабораторные работы.

Пример теста (ИОПК-4.1, ИОПК-4.3, ИОПК-9.3)

1. Какое понятие описывает информацию как предмет, который необходимо защищать?

a) Данные

b) Информация

c) Ресурс

d) Запись

2. Что из перечисленного является источником опасных сигналов?

a) Люди

b) Устройства передачи

c) Внешние помехи

d) Все вышеперечисленное

3. Какую характеристику имеет техническая разведка?

a) Секретность

b) Точность

c) Паспортизация

d) Эффективность

4. Какой канал утечки информации подразумевает использование электромагнитных волн?

a) Оптический
b) Звуковой
c) Электромагнитный
d) Вихревый

5. Что из следующего относится к средствам, предназначенным для подавления опасных сигналов?

a) Шумовые генераторы
b) Декодеры
c) Металлодетекторы
d) Акустические системы

Ключ к тесту: 1. b); 2. d); 3. b); 4. c); 5. a).

Примерные темы рефератов (ИОПК-4.1, ИОПК-4.3, ИОПК-9.3)

1. Типы микрофонных систем и их технические характеристики.
2. Лазерные акустические системы разведки.
3. Цифровые анализаторы спектра.
4. Векторные анализаторы сигналов.
5. Портативные шумомеры и вибромеры.
6. Аудиоанализаторы и область их применения.
7. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
8. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
9. Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
10. Индикаторы электромагнитного поля.
11. Сканирующие радиоприемники.
12. Специальные поисковые приемники ближней зоны и интерсепторы.
13. Программно-аппаратные комплексы радиомониторинга.
14. Анализаторы проводных линий.
15. Программно-аппаратные комплексы для исследования проводных линий.
16. Нелинейные радиолокаторы.
17. Рентгенотелевизионные комплексы.
18. Портативные металлоискатели.
19. Эндоскопы.
20. Нормативно-методические документы ФСТЭК в области технической защиты информации.

Темы лабораторных работ (ИОПК-4.1, ИОПК-4.2, ИОПК-4.3, ИОПК-9.3, ИПК-2.1)

1. Анализ технических средств перехвата информации
2. Моделирование технических каналов утечки информации

Критерии оценивания теста: тест считается выполненным при правильных ответах на более 60% вопросов.

Критерии оценивания реферата:

Процедура формирования оценки за реферат («зачтено»/ «не зачтено») включает степень самостоятельности студента при знакомстве с теоретической базой фундаментальных знаний по отдельным разделам дисциплины (по предложенной теме), полноту раскрытия темы, уровень обобщения собранного материала и отношение автора реферата к рассматриваемой проблеме и путям её решения.

Критерии оценивания лабораторных работ:

«Зачтено» – студент в целом хорошо разбирается в задаче, знает и использует методы решения практически самостоятельно или при подсказке преподавателя, отвечает на вопросы, возможно с негрубыми ошибками. Представляет работу на защите в целом хорошо, с несущественными замечаниями.

«Не зачтено» – студент слабо разбирается в задаче, не знает или знает плохо методы решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

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

Зачет проводится при положительных результатах текущего контроля, положительных ответах на теоретические вопросы и сдаче реферата и доклада по одной из предложенных преподавателем тем.

Примеры теоретических вопросов (ИОПК-4.1, ИОПК-4.3, ИОПК-9.3, ИПК-2.1)

1. Определите понятийный аппарат, связанный с защитой информации от утечек.
2. Каким образом информация может рассматриваться как объект защиты?
3. Назовите основные источники опасных сигналов и их характеристики.
4. Каковы основополагающие требования к технической разведке?
5. Опишите основные технические каналы утечки информации.
6. Какие факторы влияют на распространение сигналов в технических каналах?
7. Объясните методы подавления опасных сигналов.
8. Перечислите средства технической разведки и их функции.
9. Каковы принципы работы аппаратных средств защиты и взлома?
10. Опишите средства радиомониторинга и их назначения.
11. Каковы требования к средствам инженерной защиты объектов?
12. Назовите методы предотвращения утечки информации по техническим каналам.
13. В чем заключается принцип работы обнаружителей пустот?
14. Чем отличаются оптические каналы утечки информации от других видов?
15. Как оценивается эффективность средств защиты информации от утечек?
16. Опишите примеры применения технических средств в защите информации.
17. Как реагировать на выявленные утечки информации?
18. Какой подход следует использовать для обучения персонала по защите информации?
19. Какие права и обязанности имеют организации в области защиты информации?
20. Каковы тенденции в развитии технологий защиты информации от утечек?

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

Пример теста (ИОПК-4.1, ИОПК-4.3, ИОПК-9.3)

1. Какое понятие описывает информацию как предмет, который необходимо защищать?

a) Данные
b) Информация
c) Ресурс
d) Запись

2. Что из перечисленного является источником опасных сигналов?

a) Люди
b) Устройства передачи
c) Внешние помехи
d) Все вышеперечисленное

3. Какую характеристику имеет техническая разведка?

a) Секретность
b) Точность
c) Паспортизация
d) Эффективность

4. Какой канал утечки информации подразумевает использование электромагнитных волн?

a) Оптический
b) Звуковой
c) Электромагнитный
d) Вихревый

5. Что из следующего относится к средствам, предназначенным для подавления опасных сигналов?

a) Шумовые генераторы
b) Декодеры
c) Металлодетекторы
d) Акустические системы

Ключ к тесту: 1. b); 2. d); 3. b); 4. c); 5. a).

Информация о разработчиках

Беляев Виктор Афанасьевич, канд. техн. наук, доцент, каф. компьютерной безопасности НИ ТГУ.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент каф. компьютерной безопасности НИ ТГУ.