

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)



УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Техническая защита информации

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **10.03.01 Информационная безопасность**

Направленность (профиль): **Безопасность автоматизированных систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **4**

Семестр: **7**

Учебный план набора 2016 года

Распределение рабочего времени

| № | Виды учебной деятельности | 7 семестр | Всего | Единицы |
|---|------------------------------|-----------|-------|---------|
| 1 | Лекции | 28 | 28 | часов |
| 2 | Практические занятия | 18 | 18 | часов |
| 3 | Лабораторные работы | 36 | 36 | часов |
| 4 | Всего аудиторных занятий | 82 | 82 | часов |
| 5 | Из них в интерактивной форме | 22 | 22 | часов |
| 6 | Самостоятельная работа | 26 | 26 | часов |
| 7 | Всего (без экзамена) | 108 | 108 | часов |
| 8 | Подготовка и сдача экзамена | 36 | 36 | часов |
| 9 | Общая трудоемкость | 144 | 144 | часов |
| | | 4.0 | 4.0 | 3.Е |

Экзамен: 7 семестр

Томск 2017

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры « ___ » _____ 20__ года, протокол № _____.

Разработчик:

Старший преподаватель каф.
КИБЭВС

_____ Г. А. Праскурин

Заведующий обеспечивающей каф.
КИБЭВС

_____ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ

_____ Е. М. Давыдова

Заведующий выпускающей каф.
КИБЭВС

_____ А. А. Шелупанов

Эксперт:

Доцент кафедра КИБЭВС, ТУСУР

_____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях.

1.2. Задачи дисциплины

– Задачи дисциплины – дать основы: выявление на объекте информатизации или в выделенном помещении технических каналов утечки информации; оценка уровня шумов/информативных сигналов/помех; оценка соответствия объекта информатизации или выделенного помещения требованиям по безопасности от утечки информации по техническим каналам

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.Б.9) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Основы информационной безопасности, Управление средствами защиты информации, Физика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

– ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

В результате изучения дисциплины студент должен:

– **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации.

– **владеть** методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|--------------------------------|-------------|-----------|
| | | 7 семестр |
| Аудиторные занятия (всего) | 82 | 82 |
| Лекции | 28 | 28 |
| Практические занятия | 18 | 18 |
| Лабораторные работы | 36 | 36 |
| Из них в интерактивной форме | 22 | 22 |
| Самостоятельная работа (всего) | 26 | 26 |

| | | |
|---|-----|-----|
| Оформление отчетов по лабораторным работам | 9 | 9 |
| Проработка лекционного материала | 11 | 11 |
| Подготовка к практическим занятиям, семинарам | 6 | 6 |
| Всего (без экзамена) | 108 | 108 |
| Подготовка и сдача экзамена | 36 | 36 |
| Общая трудоемкость ч | 144 | 144 |
| Зачетные Единицы | 4.0 | 4.0 |

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|--|--------|----------------------|---------------------|------------------------|-------------------------------|-------------------------|
| 7 семестр | | | | | | |
| 1 Концепция инженерно-технической защиты информации | 4 | 0 | 0 | 2 | 6 | ПК-5, ПК-6 |
| 2 Теоретические основы инженерно-технической защиты информации | 6 | 0 | 0 | 2 | 8 | ПК-5, ПК-6 |
| 3 Физические основы защиты информации | 6 | 6 | 0 | 5 | 17 | ПК-5, ПК-6 |
| 4 Технические средства добывания и инженерно-технической защиты информации | 8 | 0 | 36 | 12 | 56 | ПК-5, ПК-6 |
| 5 Организационные основы инженерно-технической защиты информации | 2 | 6 | 0 | 2 | 10 | ПК-5, ПК-6 |
| 6 Методическое обеспечение инженерно-технической защиты информации | 2 | 6 | 0 | 3 | 11 | ПК-5, ПК-6 |
| Итого за семестр | 28 | 18 | 36 | 26 | 108 | |
| Итого | 28 | 18 | 36 | 26 | 108 | |

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоёмкость, ч | Формируемые компетенции |
|--|--|-----------------|-------------------------|
| 7 семестр | | | |
| 1 Концепция инженерно-технической защиты информации | Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации. | 2 | ПК-5, ПК-6 |
| | Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами. | 2 | |
| | Итого | 4 | |
| 2 Теоретические основы инженерно-технической защиты информации | Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре. Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации. | 1 | ПК-5, ПК-6 |
| | Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации техниче- | 2 | |

| | | | |
|---------------------------------------|---|---|------------|
| | <p>ской разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.</p> | | |
| | <p>Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов. Модели злоумышленников. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.</p> | 2 | |
| | <p>Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.</p> | 1 | |
| | Итого | 6 | |
| 3 Физические основы защиты информации | <p>Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Источники побочных излучений, их физическая природа. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.</p> | 2 | ПК-5, ПК-6 |
| | Распространение сигналов в техниче- | 1 | |

| | | | |
|--|--|---|------------|
| | ских каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах. | | |
| | Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации. | 1 | |
| | Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами. | 2 | |
| | Итого | 6 | |
| 4 Технические средства добывания и инженерно-технической защиты информации | Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки. | 2 | ПК-5, ПК-6 |
| | Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны. | 4 | |

| | | | |
|--|---|---|------------|
| | Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрывание акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления. | 2 | |
| | Итого | 8 | |
| 5 Организационные основы инженерно-технической защиты информации | Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации. | 2 | ПК-5, ПК-6 |
| | Итого | 2 | |
| 6 Методическое обеспечение инженерно-технической защиты информации | Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирова- | 2 | ПК-5, ПК-6 |

| | | | |
|------------------|--|----|--|
| | <p>ния объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации. Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.</p> | | |
| | Итого | 2 | |
| Итого за семестр | | 28 | |

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | | | |
|--|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Предшествующие дисциплины | | | | | | |
| 1 Основы информационной безопасности | + | + | | | + | + |
| 2 Управление средствами защиты информации | | | | + | + | + |
| 3 Физика | | + | + | | | |
| Последующие дисциплины | | | | | | |
| 1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | | + | | + | + | + |

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| | Виды занятий | Формы контроля |
|--|--------------|----------------|
|--|--------------|----------------|

| Компетенции | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | |
|-------------|--------|----------------------|---------------------|------------------------|--|
| ПК-5 | + | + | + | + | Экзамен, Отчет по лабораторной работе, Опрос на занятиях, Отчет по практическому занятию |
| ПК-6 | + | + | + | + | Экзамен, Отчет по лабораторной работе, Опрос на занятиях, Отчет по практическому занятию |

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

| Методы | Интерактивные практические занятия | Интерактивные лабораторные занятия | Интерактивные лекции | Всего |
|--|------------------------------------|------------------------------------|----------------------|-------|
| 7 семестр | | | | |
| Мини-лекция | | | 2 | 2 |
| IT-методы | | | 4 | 4 |
| Презентации с использованием интерактивной доски с обсуждением | | | 2 | 2 |
| Работа в команде | | 4 | | 4 |
| Решение ситуационных задач | | 4 | | 4 |
| Case-study (метод конкретных ситуаций) | | 2 | | 2 |
| Презентации с использованием видеофильмов с обсуждением | 4 | | | 4 |
| Итого за семестр: | 4 | 10 | 8 | 22 |
| Итого | 4 | 10 | 8 | 22 |

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|--|---|--------------------|----------------------------|
| 7 семестр | | | |
| 4 Технические средства добывания и инженерно-технической защиты информации | Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении. | 4 | ПК-5, ПК-6 |
| | Нелинейная локация. | 4 | |
| | Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля. | 4 | |
| | Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т». | 4 | |
| | Охрана выделенных помещений. Пожарная сигнализация. | 4 | |
| | Охрана выделенных помещений. Охранная сигнализация. | 4 | |
| | Ограничение доступа в выделенное помещение. Система контроля и управления доступом. | 4 | |
| | Охрана выделенных помещений. Система видеонаблюдения. | 8 | |
| | Итого | 36 | |
| Итого за семестр | | 36 | |

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---------------------------------------|---|--------------------|----------------------------|
| 7 семестр | | | |
| 3 Физические основы защиты информации | Моделирование систем нелинейной локации | 2 | ПК-5, ПК-6 |
| | Моделирование пассивных фильтров (низкой и высокой частоты, полосовых и режекторных фильтров) | 2 | |
| | Моделирование активных фильтров | 2 | |
| | Итого | 6 | |

| | | | |
|--|--|----|------------|
| 5 Организационные основы инженерно-технической защиты информации | Организационные мероприятия по подготовке и проведению аттестации объектов информатизации по требованиям безопасности | 6 | ПК-5, ПК-6 |
| | Итого | 6 | |
| 6 Методическое обеспечение инженерно-технической защиты информации | Методическое обеспечение проведения аттестации объектов информатизации по требованиям безопасности. Расчёт размеров опасных зон I и II | 6 | ПК-5, ПК-6 |
| | Итого | 6 | |
| Итого за семестр | | 18 | |

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|--|---|--------------------|-------------------------|--|
| 7 семестр | | | | |
| 1 Концепция инженерно-технической защиты информации | Проработка лекционного материала | 1 | ПК-5, ПК-6 | Опрос на занятиях |
| | Проработка лекционного материала | 1 | | |
| | Итого | 2 | | |
| 2 Теоретические основы инженерно-технической защиты информации | Проработка лекционного материала | 0 | ПК-5, ПК-6 | Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Проработка лекционного материала | 1 | | |
| | Проработка лекционного материала | 0 | | |
| | Итого | 2 | | |
| 3 Физические основы защиты информации | Подготовка к практическим занятиям, семинарам | 1 | ПК-5, ПК-6 | Опрос на занятиях, Отчет по практическому занятию, Экзамен |
| | Подготовка к практическим занятиям, семинарам | 1 | | |
| | Подготовка к практическим занятиям, семинарам | 1 | | |
| | Проработка лекционного материала | 0 | | |

| | | | | |
|--|---|----|---------------|--|
| | Проработка лекционного материала | 0 | | |
| | Проработка лекционного материала | 1 | | |
| | Проработка лекционного материала | 1 | | |
| | Итого | 5 | | |
| 4 Технические средства добывания и инженерно-технической защиты информации | Проработка лекционного материала | 1 | ПК-5, ПК-6 | Опрос на занятиях, Отчет по лабораторной работе, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 2 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Оформление отчетов по лабораторным работам | 1 | | |
| | Итого | 12 | | |
| 5 Организационные основы инженерно-технической защиты информации | Подготовка к практическим занятиям, семинарам | 1 | ПК-5, ПК-6 | Опрос на занятиях, Отчет по практическому занятию, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 2 | | |
| 6 Методическое обеспечение инженерно-технической защиты информации | Подготовка к практическим занятиям, семинарам | 2 | ПК-5, ПК-6 | Опрос на занятиях, Отчет по практическому занятию, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| Итого за семестр | | 26 | | |
| | Подготовка и сдача экзамена | 36 | | Экзамен |

| | | | |
|-------|----|--|--|
| Итого | 62 | | |
|-------|----|--|--|

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|--------------------------------|--|---|---|------------------|
| 7 семестр | | | | |
| Опрос на занятиях | 5 | 10 | 10 | 25 |
| Отчет по лабораторной работе | 5 | 10 | 10 | 25 |
| Отчет по практическому занятию | 5 | 5 | 10 | 20 |
| Итого максимум за период | 15 | 25 | 30 | 70 |
| Экзамен | | | | 30 |
| Нарастающим итогом | 15 | 40 | 70 | 100 |

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

| Баллы на дату контрольной точки | Оценка |
|---|--------|
| $\geq 90\%$ от максимальной суммы баллов на дату КТ | 5 |
| От 70% до 89% от максимальной суммы баллов на дату КТ | 4 |
| От 60% до 69% от максимальной суммы баллов на дату КТ | 3 |
| $< 60\%$ от максимальной суммы баллов на дату КТ | 2 |

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|--------------------------------------|--|-------------------------|
| 5 (отлично) (зачтено) | 90 - 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 - 89 | B (очень хорошо) |
| | 75 - 84 | C (хорошо) |
| | 70 - 74 | D (удовлетворительно) |
| 65 - 69 | | |
| 3 (удовлетворительно) (зачтено) | 60 - 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=176315&rnd=244973.2538529920&from=121414-0#0>
2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200126&rnd=244973.246476619&from=165971-0#0>
3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200556&rnd=244973.626813432&from=166051-0#0>
4. Торокин А. А. Инженерно-техническая защита информации. М: «Гелиос АРВ», 2005 г. 960 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.2. Дополнительная литература

1. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 1 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 150[2] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)
2. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 2 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 185[1] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)
3. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 3 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 98[2] с. : ил., табл. (наличие в библиотеке ТУСУР - 81 экз.)
4. Радиоэлектронная разведка и радиомаскировка : / В. П. Демин, А. И. Куприянов, А. В. Сахаров. - М. : МАИ, 1997. - 155, [1] с. : ил., табл. (наличие в библиотеке ТУСУР - 1 экз.)
5. Защита и охрана личности, собственности, информации : Справочное пособие / Алексей Васильевич Петраков. - М. : Радио и связь, 1997. - 320 с. : ил. (наличие в библиотеке ТУСУР - 11 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1017>, дата обращения: 30.05.2017.
2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 77 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1826>, дата обращения: 30.05.2017.
3. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2261>, дата обращения: 30.05.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. <http://portal.tusur.ru>; <http://www.lib.tusur.ru> – образовательный портал университета;
2. <http://www.iqlib.ru> – электронная интернет-библиотека;
3. <http://www.biblioclub.ru> – полнотестовая электронная библиотека;
4. <http://www.elibrary.ru> – научная электронная библиотека;
5. <http://www.edu.ru> – веб-сайт системы федеральных образовательных порталов.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Дисплейный класс с локальной вычислительной сетью и доступом в сеть Интернет Интерактивная доска с лицензионным программным обеспечением и мультимедиа-проектор

13.1.3. Материально-техническое обеспечение для лабораторных работ

Интерактивная доска с лицензионным программным обеспечением и мультимедиа-проектор Лаборатория технической защиты информации Лаборатория технических средств охраны

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеомониторов для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

| Категории студентов | Виды дополнительных оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|--|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)**

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«__» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Техническая защита информации

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **10.03.01 Информационная безопасность**

Направленность (профиль): **Безопасность автоматизированных систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **4**

Семестр: **7**

Учебный план набора 2016 года

Разработчик:

– Старший преподаватель каф. КИБЭВС Г. А. Праскурин

Экзамен: 7 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенций |
|------|---|---|
| ПК-6 | способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | Должен знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.; Должен уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации. ; |
| ПК-5 | способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | Должен владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. ; |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|-------------------------------|---|---|--|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования | Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем |
| Удовлетворительно (пороговый) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми | Работает при прямом наблюдении |

| | | | |
|----------|--|------------------------------|--|
| уровень) | | для выполнения простых задач | |
|----------|--|------------------------------|--|

2 Реализация компетенций

2.1 Компетенция ПК-6

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|----------------------------------|--|--|--|
| Содержание этапов | технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. | анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. | методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации. |
| Виды занятий | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; |
| Используемые средства оценивания | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Экзамен; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---------------------------|---|--|---|
| Отлично (высокий уровень) | <ul style="list-style-type: none"> • Физические основы, количественные и качественные характеристики технических каналов | <ul style="list-style-type: none"> • Умеет анализировать и оценивать угрозы информационной безопасности объекта от раз- | <ul style="list-style-type: none"> • Свободно владеет разными методами и средствами выявления угроз безопасности ав- |

| | | | |
|---------------------------------------|---|---|--|
| | утески информации, методы оценки эффективности технических разведок, методы оценки эффективности защиты информации от утечки по техническим каналам.; | личных источников. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем с повышенными требованиями по безопасности информации.; | томатизированным системам. Свободно владеет несколькими методами технической защиты информации. Свободно использует методы расчета и инструментального контроля показателей технической защиты информации.; |
| Хорошо (базовый уровень) | <ul style="list-style-type: none"> Знает характеристики технических каналов утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.; | <ul style="list-style-type: none"> Применяет базовые методы анализа и оценки угрозы информационной безопасности объекта. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.; | <ul style="list-style-type: none"> Может применять и обосновывать методы и средствами выявления угроз безопасности автоматизированным системам, методы технической защиты информации, методы расчета и инструментального контроля показателей технической защиты информации.; |
| Удовлетворительно (пороговый уровень) | <ul style="list-style-type: none"> Дает определения основных понятий технических каналов утечки информации, технических разведок.; | <ul style="list-style-type: none"> Умеет работать со справочной литературой. Решает типовые задачи ; | <ul style="list-style-type: none"> Может применять некоторые методы и средства выявления угроз безопасности автоматизированным системам, методы технической защиты информации.; |

2.2 Компетенция ПК-5

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|-------------------|--|---|---|
| Содержание этапов | технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. | анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации. | методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. |

| | | | |
|----------------------------------|--|--|---|
| Виды занятий | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; |
| Используемые средства оценивания | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Экзамен; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---------------------------|---|---|---|
| Отлично (высокий уровень) | <ul style="list-style-type: none"> • Физические основы, количественные и качественные характеристики технических каналов утечки информации, методы оценки эффективности технических разведок, методы оценки эффективности защиты информации от утечки по техническим каналам.; | <ul style="list-style-type: none"> • Умеет анализировать и оценивать угрозы информационной безопасности объекта от различных источников. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем с повышенными требованиями по безопасности информации.; | <ul style="list-style-type: none"> • Свободно владеет разными методами и средствами выявления угроз безопасности автоматизированным системам. Свободно владеет методами формирования требований по защите информации. Свободно использует методы расчета и инструментального контроля показателей технической защиты информации. ; |
| Хорошо (базовый уровень) | <ul style="list-style-type: none"> • Знает характеристики технических каналов утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.; | <ul style="list-style-type: none"> • Применяет базовые методы анализа и оценки угрозы информационной безопасности объекта. Пользуется нормативными документами по защите информации. ; | <ul style="list-style-type: none"> • Может применять и обосновывать методы и средствами выявления угроз безопасности автоматизированным системам. Может обосновывать методы формирования требований по защите информации. Может применять и обосновывать методы расчета и инструменталь- |

| | | | |
|---------------------------------------|---|---|---|
| | | | ного контроля показателей технической защиты информации. ; |
| Удовлетворительно (пороговый уровень) | <ul style="list-style-type: none"> • Дает определения основных понятий технических каналов утечки информации, технических разведок.; | <ul style="list-style-type: none"> • Умеет работать со справочной литературой. Решает типовые задачи ; | <ul style="list-style-type: none"> • Может применять некоторые методы и средствами выявления угроз безопасности автоматизированным системам, методы формирования требований по защите информации.; |

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Темы опросов на занятиях

– Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.

– Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.

– Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.

– Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.

– Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

– Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.

– Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов. Модели злоумышленников. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.

– Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

– Физические основы побочных электромагнитных излучений и наводок. Акустоэлектри-

ческие преобразования. Источники побочных излучений, их физическая природа. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

– Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах.

– Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.

– Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

– Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

– Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

– Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрывание акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.

– Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

– Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

– Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

– Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

3.2 Экзаменационные вопросы

- 1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации.
- 2. Классификация технической разведки. Эффективность добывания информации технической разведкой.
- 3. Государственная система защиты информации. Эффективность защиты информации.
- 4. Основные объекты защиты информации.
- 5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.
- 6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2.
- 7. Состав технического канала утечки информации.
- 8. Классификация технических каналов утечки информации.
- 9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.
- 10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.
- 11. Перечислите каналы утечки речевой информации. Приведите примеры.
- 12. Перечислите каналы утечки видовой информации. Приведите примеры.
- 13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах связи.
- 14. Перечислите методы противодействия утечке информации по техническим каналам.
- 15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.
- 16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.
- 17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».
- 18. Направленные микрофоны. Принцип действия.
- 19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.
- 20. Датчики охранных систем. Принципы действия датчиков.
- 21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.
- 22. Средства радиотехнической разведки. Состав. Характеристики.
- 23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.
- 24. Периметровые средства охраны. Датчики периметровых систем охраны.
- 25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.
- 26. Экранирование электромагнитных волн.
- 27. Экранирование акустических сигналов.
- 28. Фильтрация опасных сигналов. Приведите примеры.
- 29. Маскировка опасных сигналов зашумлением. Приведите примеры.
- 30. Металлодетекторы. Сферы применения. Принцип действия.
- 31. Локаторы нелинейностей. Сферы применения. Принцип действия.
- 32. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.
- 33. Специальная проверка. Специальное обследование. Специальное исследование.
- 34. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.
- 35. Проведение измерений побочных электромагнитных излучений. Приведите примеры.

3.3 Вопросы для подготовки к практическим занятиям, семинарам

- Моделирование систем нелинейной локации
- Моделирование пассивных фильтров (низкой и высокой частоты, полосовых и режекторных фильтров)
- Моделирование активных фильтров
- Организационные мероприятия по подготовке и проведению аттестации объектов информатизации по требованиям безопасности
- Методическое обеспечение проведения аттестации объектов информатизации по требованиям безопасности. Расчёт размеров опасных зон I и II

3.4 Темы лабораторных работ

- Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.
- Нелинейная локация.
- Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.
- Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т».
- Охрана выделенных помещений. Пожарная сигнализация.
- Охрана выделенных помещений. Охранная сигнализация.
- Ограничение доступа в выделенное помещение. Система контроля и управления доступом.
- Охрана выделенных помещений. Система видеонаблюдения.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=176315&rnd=244973.2538529920&from=121414-0#0>
2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200126&rnd=244973.246476619&from=165971-0#0>
3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200556&rnd=244973.626813432&from=166051-0#0>
4. Торокин А. А. Инженерно-техническая защита информации. М: «Гелиос АРВ», 2005 г. 960 с. (наличие в библиотеке ТУСУР - 30 экз.)

4.2. Дополнительная литература

1. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 1 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 150[2] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)
2. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 2 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 185[1] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

3. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 3 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 98[2] с. : ил., табл. (наличие в библиотеке ТУСУР - 81 экз.)

4. Радиоэлектронная разведка и радиомаскировка : / В. П. Демин, А. И. Куприянов, А. В. Сахаров. - М. : МАИ, 1997. - 155, [1] с. : ил., табл. (наличие в библиотеке ТУСУР - 1 экз.)

5. Защита и охрана личности, собственности, информации : Справочное пособие / Алексей Васильевич Петраков. - М. : Радио и связь, 1997. - 320 с. : ил. (наличие в библиотеке ТУСУР - 11 экз.)

4.3. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1017>, свободный.

2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 77 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1826>, свободный.

3. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2261>, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. <http://portal.tusur.ru>; <http://www.lib.tusur.ru> – образовательный портал университета;

2. <http://www.iqlib.ru> – электронная интернет-библиотека;

3. <http://www.biblioclub.ru> – полнотестовая электронная библиотека;

4. <http://www.elibrary.ru> – научная электронная библиотека;

5. <http://www.edu.ru> – веб-сайт системы федеральных образовательных порталов.