Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

Б.1.3.10.2 «Технические каналы утечки информации на объектах информатизации»

направления подготовки
10.03.01«Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72
в том числе:
лекции – 16
практические занятия – 18
самостоятельная работа – 36
коллоквиум - 2
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов методам, технологиям и применению специальных технических средств для защиты информации от ведения технической разведки.

Задачи изучения дисциплины:

- изучить общие принципы организации инженерно-технической защиты информации
- изучить основные методы ведения технической разведки и методы противодействия технической разведке, научиться определять преимущества и недостатки этих методов в рамках решения конкретных задач по защите информации
- получить практические навыки по организации комплексных работ по инженерно-технической защите информации
- научиться применять технические средства для проведения мероприятий по инженерно-технической защите информации
- научиться применять инструментальные средства для оценки эффективности мероприятий по противодействия технической разведке

2. Место дисциплины в структуре ООП ВО

Дисциплина «Техническая защита информации» относится к числу дисциплин базовой (общепрофессиональной) части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Физика» - знать физическую природу электромагнитных и акустических колебаний и волн, оптику, основы электромагнетизма, основы теории измерений

цикл математических дисциплин — знать и уметь применять методы анализа функций, основы интегрального и дифференциального исчисления, основы векторного анализа и алгебры, теорию вероятностей и мат. статистики, знать и уметь строить и анализировать математические модели объектов различной природы, а также использовать методы численного анализа для исследования построенных моделей

«Электроника и схемотехника», «Основы радиотехники» – знать основные средства и способы электромагнитной передачи информации, основы теории цепей, основы электродинамики и распространения радиоволн, основы теории радиопередающих и радиоприемных устройств.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-5 - способность использовать нормативные правовые акты в своей профессиональной деятельности

ОПК-7 - способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Студент должен знать:

1. общие принципы организации инженерно-технической защиты конфиденциальной информации
2. основные технические каналы утечки информации и их свойства
3. физические и физико-технические основы реализации технических каналов утечки информации
4. математические модели, методы и подходы к описанию физических и физико-технических явлений, возникающих при реализации технических каналов утечки информации
5. возможности основных методов ведения технической разведки конфиденциальной информации
6. основные требования отраслевых и распорядительных нормативных документов по технической защите информации

Студент должен уметь:

1. оценивать степень опасности технических каналов утечки конфиденциальной информации
2. применять специальные технические средства для проведения мероприятий по инженерно-технической защите информации
3. оценивать степень опасности технических каналов утечки конфиденциальной информации
4. блокировать основные технические каналы утечки информации
5. проводить математическое моделирование и теоретический анализ технических каналов утечки информации

Студент должен владеть:

1. методиками и способами инструментальной оценки степени опасности технических каналов утечки конфиденциальной информации на объекте информатизации
2. методиками проведения инструментальной оценки эффективности мероприятий по блокированию основных технических каналов утечки информации

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ мо-ду-ля	№ неде-ли	№ те-мы	Наименование темы	Часы/ Из них в интерактивной форме				
				Всего	Лек-ции	Коллок виум	Прак-тичес -кие	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
8 семестр								
1	1-4	1	Введение. Техническая разведка: разновидности, специфика, возможности	13/2	4/2	-	-	9
1	5-8	2	Информация, носители информации, каналы утечки информации. Сигналы как носители информации.	19/3	4/2	2	6/1	9
2	9-12	3	Опасные сигналы и информативные поля. Специальные технические средства негласного получения информации	19/3	4/2	-	6/1	9
2	13-18	4	Инженерно-техническая защита информации	19/2	4/1	-	6/1	9
Всего				72 /10	16/6	2	18/3	36

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Литература
1	4	**1,2**	Введение. Классификация технической разведки. Нормативные документы по противодействию технической разведке. Характеристика государственной системы противодействия технической разведке конфиденциальной информации. Юридические аспекты задач технической защиты информации	1-3, 4, 9
2	4	3,4	Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Виды, источники и носители защищаемой информации. Концепция и методы инженерно-технической защиты информации. Структура, классификация и основные характеристики технических каналов утечки информации	1-3, 5,7, 9, 10-22
3	4	**5,6**	Опасные сигналы и их источники. Побочные	1, 4, 6, 8, 10-22

			электромагнитные излучения и наводки. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Скрытое получение информации при помощи специальных технических средств. Демаскирующие признаки объектов наблюдения и сигналов. Скрытие объектов наблюдения. Обнаружение и локализация закладных устройств, подавление их сигналов	
4	4	**7,8**	Основные положения методологии инженерно-технической защиты информации. Методы и средства инженерной защиты и технической охраны объектов. Виды контроля эффективности защиты информации. Методы расчета и инструментального контроля показателей защиты информации.	1-3, 4, 9, 10-22

6. Содержание коллоквиумов

№ темы	Темы, выносимые на коллоквиум	Литература
1	Введение. Классификация технической разведки. Нормативные документы по противодействию технической разведке. Характеристика государственной системы противодействия технической разведке конфиденциальной информации. Юридические аспекты задач технической защиты информации	1-3, 4, 9
2	Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Виды, источники и носители защищаемой информации. Концепция и методы инженерно-технической защиты информации. Структура, классификация и основные характеристики технических каналов утечки информации	1-3, 5,7, 9, 10-22

7. Перечень лабораторных работ

Лабораторные работы учебным планом не предусмотрены.

8. Перечень практических занятий

№ темы	Всего часов	Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Литература
1-3	12	ИССЛЕДОВАНИЕ СВОЙСТВ И ХАРАКТЕРИСТИК ТЕХНИЧЕСКИХ УСТРОЙСТВ СКРЫТНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ	1-3, 4, 9

2,3	8	ИССЛЕДОВАНИЕ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК И МЕТОДОВ ОРГАНИЗАЦИИ РАДИОМОНИТОРИНГА ПРИ ПОМОЩИ ПОИСКОВО-РАЗВЕДЫВАТЕЛЬНОГО КОМПЛЕКСА Р-375 «Кайра»	1-3, 5,7, 9, 10-26
3,4	8	МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. Подавление электроакустического канала утечки информации и предотвращение прослушивания телефонных линий	1, 4, 6, 8, 10-26
1-4	8	ПРАКТИКА РАДИОМОНИТОРИНГА	1-3, 4, 9, 10-26

9. Задания для самостоятельной работы студентов

№ темы	Всего часов	Вопросы для самостоятельного изучения (задания)	Литература
1	12	Возможности видов технической разведки.	1-3, 4, 9
2	12	Основные этапы и процедуры добывания информации технической разведкой.	1-3, 5,7, 9, 10-26
3	12	Структура, классификация и основные характеристики технических каналов утечки информации. Опасные сигналы и их источники.	1, 4, 6, 8, 10-26
4	18	Скрытое получение информации при помощи специальных технических средств	1-3, 4, 9, 10-26

Виды, график контроля СРС (по решению кафедры УМКС/УМКН)

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
8 семестр			
1-2	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	промежуточная аттестация (8)
3-4	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	зачет

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [26].

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Курсовой проект учебным планом не предусмотрен.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Вопросы для экзамена

Экзамен учебным планом не предусмотрен.

Вопросы для зачета

1. Классификация технической разведки.
2. Виды, источники и носители защищаемой информации.
3. Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой
4. Концепция и методы инженерно-технической защиты информации.
5. Нормативные документы по противодействию технической разведке. Характеристика государственной системы противодействия технической разведке
6. Структура, классификация и основные характеристики технических каналов утечки информации.
7. Визуально-оптический технический канал утечки информации
8. Опасные сигналы и их источники
9. Материально-вещественный технический канал утечки информации
10. Классификация технической разведки.
11. Виброакустический технический канал утечки информации
12. Электромагнитный технический канал утечки информации
13. ПЭМиН канал утечки информации
14. Маскировка и шифрование речевой информации в каналах связи. Современные тенденции в построении систем скремблирования
15. Энергетическая маскировка акустических информативных сигналов
16. Подавление опасных сигналов акустоэлектрических преобразователей
17. Экранирование и компенсация информативных полей.
18. Подавление информативных сигналов в цепях заземления и электропитания
19. Скрытое получение информации при помощи специальных технических средств.
20. Юридические и технические аспекты классификации и экспертизы СТС
21. Демаскирующие признаки объектов наблюдения и источников опасных сигналов. Скрытие объектов наблюдения

22. Разновидности закладных устройств. Обнаружение и локализация закладных устройств, подавление их сигналов

23. Радиомониторинг. Технические средства для ведения радиомониторинга. Организация радиомониторинга на объекте информатизации

24. Техническое обеспечение процедур радиомониторинга. Поисково-слежечные и контрольные РПУ, анализаторы спектра, сканирующие РПУ, селективные микровольтметры, детекторы поля

25. Основные положения методологии инженерно-технической защиты информации. Методы и средства инженерной защиты

26. Технические средства блокирования визуально-оптического и материально-вещественного технических каналов утечки информации

27. Блокирование виброакустического технического канала утечки информации. Генераторы вибрационного и акустического зашумления - характеристики, особенности применения, примеры моделей

28. Блокирование электромагнитного технического канала утечки информации. Генераторы пространственного и линейного электромагнитного зашумления - характеристики, особенности применения, примеры моделей

29. Защита телефонных и проводных линий связи. Пассивные средства и методы защиты

30. Блокирование технического канала ПЭМиН. Классификация и характеристики ОТСС и ВТСС. Пассивные и активные средства защиты и противодействия

31. Виды контроля эффективности защиты информации. Методы расчета и инструментального контроля показателей защиты информации на объекте информатизации

32. Нелинейная локация (NLJD) как способ обнаружения СТС. Теория, практическая реализация, характеристики приборов, возможные ограничения

33. Типовые измерения при оценке ЭМ и ПЭМиН технических каналов. Оценка опасных зон объекта информатизации

34. Типовые измерения при оценке виброакустического канала на объекте информатизации

35. Подготовка объекта информатизации к процедуре лицензирования: требования РД СТР-К

36. Разработка и оформление комплекта типовой документации для лицензирования объекта информатизации. Шаблоны документов

37. Процедурные вопросы лицензирования объекта информатизации. Организация работы службы (отдела) защиты конфиденциальной информации

38. Применение современных методов защиты конфиденциальной информации. Secure communications by chaotic signals

39. Современные тенденции защиты конфиденциальной информации за рубежом. TSCM

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы с описанием показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Формирование профессиональных компетенций по дисциплине производится на лабораторных и лекционных занятиях (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче зачета (15%).

Итоговое оценивание усвоения дисциплины осуществляется путем приема зачета. Результаты зачета оцениваются «зачтено» и «незачтено».

При выставлении оценок преподаватель руководствуется следующим:

- оценки «зачтено» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе, продемонстрировавший умения и навыки в рамках формируемых компетенций на хорошем уровне освоения, способный к самостоятельному пополнению знания в ходе дальнейшей учебной работы и профессиональной деятельности;

- оценка «незачтено» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившего принципиальные ошибки в выполнении предусмотренных программой заданий, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «незачтено» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ПК-7

Наименование компетенции

Индекс ПК-7	Формулировка: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	Знает: - основные технические каналы утечки информации и их свойства; Умеет: - применять специальные технические средства для проведения мероприятий по инженерно-технической защите информации; Владеет: - методиками и способами инструментальной оценки степени опасности технических каналов утечки конфиденциальной информации на объекте информатизации;
Продвинутый (хорошо)	Знает: - основные технические каналы утечки информации и их свойства; - физические и физико-технические основы реализации технических каналов утечки

	информации; Умеет: - оценивать степень опасности технических каналов утечки конфиденциальной информации; - применять специальные технические средства для проведения мероприятий по инженерно-технической защите информации; Владеет: - методиками и способами инструментальной оценки степени опасности технических каналов утечки конфиденциальной информации на объекте информатизации;
Высокий (отлично)	Знает:- основные технические каналы утечки информации и их свойства; - физические и физико-технические основы реализации технических каналов утечки информации; - математические модели, методы и подходы к описанию физических и физико-технических явлений, возникающих при реализации технических каналов утечки информации; - возможности основных методов ведения технической разведки конфиденциальной информации; Умеет: - оценивать степень опасности технических каналов утечки конфиденциальной информации; - применять специальные технические средства для проведения мероприятий по инженерно-технической защите информации; - проводить математическое моделирование и теоретический анализ технических каналов утечки информации Владеет: - методиками и способами инструментальной оценки степени опасности технических каналов утечки конфиденциальной информации на объекте информатизации; - методиками проведения инструментальной оценки эффективности мероприятий по блокированию основных технических каналов утечки информации

УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ОПК-5

Наименование компетенции

Индекс	Формулировка:
ОПК-5	способность использовать нормативные правовые акты в своей профессиональной деятельности

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	Знает: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; Умеет: - анализировать и оценивать угрозы информационной безопасности объекта; Владеет: - навыками работы с нормативными правовыми актами; - методами формирования требований по защите информации; - профессиональной терминологией.
Продвинутый (хорошо)	Знает: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Умеет: - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; Владеет: - навыками работы с нормативными правовыми актами; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и контроля показателей технической защиты информации; - профессиональной терминологией.

Высокий (отлично)	Знает: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Умеет: - 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; Владеет: - навыками работы с нормативными правовыми актами; - методами и средствами выявления угроз безопасности; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и контроля показателей технической защиты информации; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией.

УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ОПК-7

Наименование компетенции

Индекс	Формулировка:
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	Знает: - основные законодательные и нормативные документы по защите информации техническими средствами; - правовые основы деятельности подразделений защиты информации; - физические и технические основы защиты информации; - возможности перехвата информации техническими средствами; - основные способы инженерно-технической защиты информации; - принципы и методы организационной защиты информации; - физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; - формы и способы представления данных в персональном компьютере; Умеет: - самостоятельно анализировать и оценивать факты, явления и события; - раскрывать причинно-следственные связи между фактами, явлениями и событиями; - использовать методы научной абстракции для анализа явлений и процессов; - раскрывать закономерную связь исходного отношения с его различными проявлениями; - пользоваться современной научно-технической литературой, нормативными и методическими материалами по инженерно-технической защите объектов информатизации; - описывать объекты защиты; - анализировать и оценивать угрозы информационной безопасности объекта; - решать типовые прикладные физические задачи; Владеет: - методами формирования требований по защите информации; - навыками обеспечения безопасности информации с помощью типовых программных и технических средств; - навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты
Продвинутый	Знает: - основные законодательные и нормативные документы по защите информации техническими средствами;

(хорошо)	- правовые основы деятельности подразделений защиты информации; - физические и технические основы защиты информации; - основные демаскирующие признаки объектов защиты; - возможности перехвата информации техническими средствами; - методы защиты информации техническими средствами и методы оценки их эффективности; - основные способы инженерно-технической защиты информации; - принципы работы технических средств защиты и технического контроля защищенности объектов информатизации; - основные методы исследования и диагностики технических средств защиты информации; - принципы и методы организационной защиты информации; - технические каналы утечки информации; - физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; - формы и способы представления данных в персональном компьютере; Умеет: - самостоятельно анализировать и оценивать факты, явления и события; - раскрывать причинно-следственные связи между фактами, явлениями и событиями; - использовать методы научной абстракции для анализа явлений и процессов; - раскрывать закономерную связь исходного отношения с его различными проявлениями; - пользоваться современной научно-технической литературой, нормативными и методическими материалами по инженерно-технической защите объектов информатизации; - устанавливать связи между различными способами обработки информации; - описывать объекты защиты; - организовывать защиту объекта активными и пассивными способами и техническими средствами; - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - решать типовые прикладные физические задачи; Владеет: - навыками письменного аргументированного изложения собственной точки зрения; - программными средствами построения технологий обработки данных в предметной области; - методами управления использованием информационных ресурсов при передаче конфиденциальной информации по техническим каналам; - способностью самостоятельного изучения и освоения новых технических средств защиты информации; - методами технической защиты информации; - методами формирования требований по защите информации; - навыками обеспечения безопасности информации с помощью типовых программных и технических средств; - навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты
Высокий (отлично)	Знает: - основные законодательные и нормативные документы по защите информации техническими средствами; - правовые основы деятельности подразделений защиты информации; - физические и технические основы защиты информации; - основные демаскирующие признаки объектов защиты; - возможности перехвата информации техническими средствами; - активные и пассивные способы и средства сокрытия информации; - способы и средства технической дезинформации; - методы защиты информации техническими средствами и методы оценки их эффективности; - основные способы инженерно-технической защиты информации; - принципы работы технических средств защиты и технического контроля защищенности объектов информатизации; - основные методы исследования и диагностики технических средств защиты информации; - принципы и методы организационной защиты информации; - технические каналы утечки информации; - возможности технических разведок; - способы и средства защиты информации от утечек по техническим каналам; - физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; - формы и способы представления данных в персональном компьютере;

	- универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий. Умеет: - самостоятельно анализировать и оценивать факты, явления и события; - раскрывать причинно-следственные связи между фактами, явлениями и событиями; - использовать методы научной абстракции для анализа явлений и процессов; - раскрывать закономерную связь исходного отношения с его различными проявлениями; - пользоваться современной научно-технической литературой, нормативными и методическими материалами по инженерно-технической защите объектов информатизации; - проводить контроль параметров и уровня негативных воздействий применяемых технических средств на человека; - эффективно применять средства защиты от негативных воздействий; - устанавливать связи между различными способами обработки информации; - оценивать точность и достоверность полученной информации; - описывать объекты защиты; - организовывать защиту объекта активными и пассивными способами и техническими средствами; - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; - решать типовые прикладные физические задачи; - применять нормативные документы по метрологии, стандартизации и сертификации на практике. Владеет: - навыками письменного аргументированного изложения собственной точки зрения; - навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного вида рассуждений; - методами анализа методов и средств передачи, хранения и обработки данных; - навыками выбора моделей данных, моделей знаний и методов организации данных; - программными средствами построения технологий обработки данных в предметной области; - методами управления использованием информационных ресурсов при передаче конфиденциальной информации по техническим каналам; - способностью самостоятельного изучения и освоения новых технических средств защиты информации; - 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; - навыками обеспечения безопасности информации с помощью типовых программных и технических средств; - навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты

Тестовые задания по дисциплине

Для проведения тестирования используются тестовые материалы, разработанные в среде АСТ-Тест.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

Общее количество занятий, проводимых в интерактивных формах, не менее 10 часов.

15. Перечень учебно-методического обеспечения для обучающихся по дисциплине

Обязательные издания

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: http://www.iprbookshop.ru/16710.— ЭБС «IPRbooks», по паролю

2. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7000.— ЭБС «IPRbooks», по паролю

3. Разработка системы технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7005.— ЭБС «IPRbooks», по паролю

Дополнительные издания

4. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Креопалов В.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871.— ЭБС «IPRbooks», по паролю

5. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 197 с.— Режим доступа: http://www.iprbookshop.ru/13931.— ЭБС «IPRbooks», по паролю

6. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебник/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 442 с.— Режим доступа: http://www.iprbookshop.ru/12053.— ЭБС «IPRbooks», по паролю

7. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия -

Телеком, 2012.— 616 c.— Режим доступа: http://www.iprbookshop.ru/12054.— ЭБС «IPRbooks», по паролю
8. Титов А.А. Технические средства защиты информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 194 c.— Режим доступа: http://www.iprbookshop.ru/13989.— ЭБС «IPRbooks», по паролю
9. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 c.— Режим доступа: http://www.iprbookshop.ru/7008.— ЭБС «IPRbooks», по паролю
10. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю
11. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю
12. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 224 c.— Режим доступа: http://www.iprbookshop.ru/7007.— ЭБС «IPRbooks», по паролю
13. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/12048.— ЭБС «IPRbooks», по паролю
14. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ Васильев В.И.— Электрон. текстовые данные.— М.: Машиностроение, 2013.— 172 c.— Режим доступа: http://www.iprbookshop.ru/18519.— ЭБС «IPRbooks», по паролю
15. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами [Электронный ресурс]: методические указания к самостоятельной работе студентов. Учебно-методическое пособие/ Бурняшов Б.А.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 55 c.— Режим доступа: http://www.iprbookshop.ru/23077.— ЭБС «IPRbooks», по паролю

16. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю
17. Вузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс]: учебное пособие/ Вузов Г.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2010.— 240 с.— Режим доступа: http://www.iprbookshop.ru/12039.— ЭБС «IPRbooks», по паролю
18. Комарова О.И. Обучение устной речи и чтению литературы на английском языке по специальности «Защита информации». Часть 1 [Электронный ресурс]: учебно-методическое пособие/ Комарова О.И., Румянцева Е.И.— Электрон. текстовые данные.— М.: Московский государственный технический университет имени Н.Э. Баумана, 2010.— 32 с.— Режим доступа: http://www.iprbookshop.ru/31100.— ЭБС «IPRbooks», по паролю

Периодические издания

19. Информационная безопасность регионов [Текст] : науч.-техн. журнал. - Саратов : Изд-во СГСЭУ, 2007 - . - Выходит раз в два месяца. - ISSN 1995-5731
20. Цифровая обработка сигналов [Текст] : науч.-техн. журн. - М. : Рос. науч.-техн. общество радиотехники и электроники и связи им. А. С. Попова, 1999 - . - Выходит ежеквартально. - ISSN 1684-2634
21. Вестник Саратовского государственного технического университета [Текст]. : науч.-техн. журн. / Сарат. гос. техн. ун-т (Саратов); гл. ред. И. Р. Плеве. - Саратов : СГТУ. - Саратов : СГТУ, 2003. - . - Выходит ежеквартально. - ISSN 1999-8341
22. Известия вузов. Прикладная нелинейная динамика [Текст] : науч.-техн. журнал. - Саратов : Изд-во СГУ, 1993 - . - Выходит раз в два месяца. - ISSN 0869-6632

Интернет-ресурсы

23. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Режим доступа: http://fstec.ru/ Дата обращения 05.05.2015
24. Литература по цифровой обработке сигналов. Режим доступа: http://www.dsp-book.narod.ru/books.html Дата обращения 05.05.2015
25. Специальные радиосистемы. Режим доступа: http://www.radioscanner.ru Дата обращения 05.05.2015

Источники ИОС

26. Учебные материалы. Режим доступа: https://portal.sstu.ru/Fakult/FETIP/IBS/b316_1/DocLib/Forms/AllItems.aspx Дата обращения 05.02.2016

16. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

– персональный компьютер (в конфигурации не хуже: процессор Intel Core 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);

– проектор (разрешение не менее 1280x1024);

– экран для проектора

Для проведения лабораторных занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт с установленными:.

1. Операционные системы семейств Microsoft Windows 7/XP, Linux.

2. Программа математического процессинга Matlab

3. Следующее лабораторное оборудование и специальные технические средства для защиты информации, радиоэлектронное измерительное оборудование, лабораторные экспериментальные стенды и комплексы:

№ п/п	Наименование прибора	количество	инвентарный номер	примечание (дислокация)
1	Антенна ВЧ с переходником для ГРОМ ЗИ 4А	1	1381644	к.518 -А
2	Блокиратор сотовых телефонов G-Guard YK-300	2	1381638 1381639	к.518 -Б
4	Генератор TGR 1040	1	1637116	к.518 -Б
5	Генератор GFG8210	1	1380945	к.518 -Б
6	Диктофон Olimpus 400 GP	1	1330010	к.518 -Б
7	Диктофон Samsung SVR-BR-1640	1	1330011	к.518 -Б
8	Микроскоп стереоскопический МБС-9	1	-	к.518 -Б
9	Индикатор поля D006	1	1330007	к.518 -А
10	Источник питания GPS3030DD	2	1380946	к.518 -Б
11	Источник питания PPE-3323/RS	1	1361351	к.518 -Б
12	Комплекс измерительный TG 2000	1	1637114	к.518 -Б
13	Комплект измерительного оборудования на базе анализатора спектра Agilent E4405B	1	1330029	к.518 -А
14	Комплект измерительного оборудования на базе осциллографа	1	1330034	к.518 -Б

	Tektronix TDS2022			
15	Компьютер Pentium 4 3.0	1	1361376	к.518 -А
16	Компьютер Pentium 4 3.0	1	1361496	к.518 -Б
17	Осциллограф DSO3102A	1	1635611	к.518 -Б
18	Телефонный аппарат	1		к.518 -Б
19	Имитатор СТС (микровидеокамера, камуфлированная в часы)	1	-	к.518 -Б
20	Подавитель диктофонов Рамзес-Авто	1	1330008	к.518 -А
21	Прибор ГРОМ-ЗИ4 устройство защиты телефонных линий	1	1330005	к.518 -А
22	Прибор ГРОМ-ЗИ-6 устройство защиты телефонных линий	1	1330006	к.518 -А
23	Ручной измеритель частоты РИЧ-3	1	1330084	к.518 -А
24	Тест-приёмник OPTOELECTRONICS	1	1330009	к.518 -А
25	Цифровой мультиметр GDM-354	1	1380947	к.518 -Б
26	Измеритель RLC Tesla BM591	1	-	к.518 -Б
27	Генератор HAMEG HM8135	1	1647688	к.518 -Б
28	Р/п комплекс Р375	1	-	к.518 -А
29	Р/п «Волна-К»	1	-	к.518 -А
30	Радиотелефон COMO CT-98000 (базовый блок, блок абонента)	1	-	к.518 -А
31	Радиоприемник бытовой	3	-	к.518 -А
32	Приемник трехпрограммный СИБИРЯК 303	1	-	к.518 -А
33	Имитатор СТС (беспроводное закладное устройство, лаб. стенд)	1	-	к.518 -Б