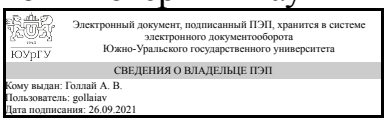
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



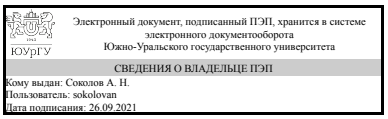
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.25 Техническая защита информации
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

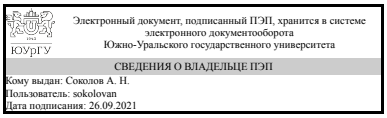
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика, к.техн.н., доц.



А. Н. Соколов

Разработчик программы, к.техн.н., доц., заведующий кафедрой



А. Н. Соколов

Челябинск

1. Цели и задачи 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. Задачами дисциплины является изучение: - технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами; - технических каналов утечки акустической (речевой) информации; - способов и средств защиты информации, обрабатываемой техническими средствами; - способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации; - методов и средств контроля эффективности защиты информации от утечки по техническим каналам; - основ организации технической защиты информации на объектах информатизации.

Краткое содержание дисциплины

1. Технические каналы утечки информации. Основные понятия и определения. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки акустической (речевой) информации. 2. Способы и средства защиты информации от утечки по техническим каналам. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. 3. Методы и средства контроля эффективности технической защиты информации. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. Методы и средства выявления электронных устройств негласного получения информации. 4. Организация технической защиты информации на объектах информатизации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:основные нормативные правовые акты в области информационной безопасности и защиты информации
	Уметь:пользоваться нормативными документами по защите информации
	Владеть:навыками работы с нормативными документами по защите информации
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Знать:технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности

	технической защиты информации
	Уметь:анализировать и оценивать угрозы информационной безопасности объекта
	Владеть:методами и средствами выявления угроз безопасности автоматизированным системам
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Знать:нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации
	Уметь:пользоваться нормативными документами по защите информации
	Владеть:методами технической защиты информации; методами формирования требований по защите информации
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Знать:технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам
	Уметь:пользоваться нормативными документами по защите информации
	Владеть:методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов
ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать:методы и средства контроля эффективности технической защиты информации
	Уметь:
	Владеть:методами расчета и инструментального контроля показателей технической защиты информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.24.02 Правовое обеспечение информационной безопасности, Б.1.32 Метрология, стандартизация и сертификация, Б.1.12 Электродинамика и распространение радиоволн, Б.1.06 Физика, Производственная практика, эксплуатационная практика (6 семестр)	Б.1.42 Измерительная аппаратура контроля защищенности объектов информатизации, В.1.08 Основы аттестации объектов информатизации критически важных объектов, Б.1.30.01 Разработка защищенных автоматизированных систем, В.1.07 Инженерно-техническая защита информации и технические средства охраны на критически важных объектах, Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности (8 семестр), Производственная практика, преддипломная практика (10 семестр)

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.12 Электродинамика и распространение радиоволн	Знать: основные понятия, уравнения и законы электродинамики и распространения радиоволн. Уметь: оценивать основные параметры электромагнитных полей. Владеть: основными методами исследования электромагнитных полей и на практике использовать эти знания для анализа физических и технических характеристик радиоэлектронных средств.
Б.1.32 Метрология, стандартизация и сертификация	Знать: физические процессы, лежащие в основе измерения различных физических величин; основные нормативные акты сертификации. Уметь: находить и определять область применения различных категорий и видов стандартов.
Б.1.24.02 Правовое обеспечение информационной безопасности	Знать: основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Уметь: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; пользоваться нормативными документами по противодействию технической разведке. Владеть: навыками работы с нормативными правовыми актами; методами формирования требований по защите информации.
Б.1.06 Физика	Знать: теорию механических и электромагнитных колебаний и волн; методы и средства измерения физических величин. Владеть: навыками обработки экспериментальных данных и оценки точности измерений.
Производственная практика, эксплуатационная практика (6 семестр)	Владеть: навыками описания и документирования объекта информатизации, подлежащего защите.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 5 з.е., 180 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	180	180
Аудиторные занятия:	80	80
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16

Самостоятельная работа (СРС)	100	100
Подготовка к лабораторным работам, оформление результатов	16	16
Курсовая работа	52	52
Подготовка к практическим занятиям, оформление результатов	32	32
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен,КР

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Технические каналы утечки информации	34	10	16	8
2	Способы и средства защиты информации от утечки по техническим каналам.	22	6	8	8
3	Методы и средства контроля эффективности технической защиты информации.	16	12	4	0
4	Организация технической защиты информации.	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия и определения.	2
2	1	Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	4
3	1	Технические каналы утечки акустической (речевой) информации.	4
4	2	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	4
5	2	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.	2
6	3	Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	4
7	3	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.	4
8	3	Методы и средства выявления электронных устройств негласного получения информации.	4
10	4	Организация технической защиты информации на объектах информатизации.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Методика оценки угроз утечки информации по оптическому каналу.	2
2	1	Методика оценки угроз утечки информации по каналу, возникающему за счет побочных электромагнитных излучений и наводок (ПЭМИН).	4
3	1	Методика оценки угроз утечки акустической (речевой) информации.	4

4	1	Технические средства разведки и перехвата информации.	2
5	1	Моделирование защищаемого объекта. Проектирование системы защиты информации объекта информатизации.	4
6	2	Средства защиты информации от утечки по каналу, возникающему за счет ПЭМИН.	4
7	2	Средства защиты информации от акустической речевой разведки (АРР).	4
8	3	Средства обнаружения технических каналов утечки информации.	4
9	4	Нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации от утечек по техническим каналам.	4

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Исследование звукоизоляции и виброизоляции защищаемого помещения.	2
2	1	Акустоэлектрические преобразования во вспомогательных средствах и системах.	2
3	1	Побочные электромагнитные излучения средств вычислительной техники.	2
4	1	Побочные электромагнитные наводки от средств вычислительной техники в линейных коммуникациях.	2
5	2	Виброакустическая защита речевой информации.	2
6	2	Защита от акустоэлектрических преобразований.	2
7	2	Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением.	2
8	2	Защита от побочных электромагнитных наводок в линейных коммуникациях.	2

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка к практическим занятиям, оформление результатов	Основная литература	32
Курсовая работа	Дополнительная литература	52
Подготовка к лабораторным работам, оформление результатов	Основная литература	16

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Использование проектно-организованных технологий обучения работе в команде над комплексным решением практических задач	Практические занятия и семинары	Студенты делятся на несколько команд, каждая из которых прячет в кабинете иммитации закладных устройств, другая команда должна найти данные макеты	2

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Выполнение и защита курсовой работы	11-13
Все разделы	ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Выполнение и защита курсовой работы	1 - 10
Все разделы	ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Экзамен	1 - 50
Все разделы	ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Экзамен	1 - 50
Все разделы	ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Экзамен	1 - 50

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Экзамен	Студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает 2 теоретических вопроса по пройденным разделам. Преподаватель проверяет, беседует и оценивает.	Отлично: обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы. Хорошо: знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. Удовлетворительно: знает только основной

		материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности в изложении материала. Неудовлетворительно: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.
Выполнение и защита курсовой работы	Преподаватель проверяет и оценивает выполнение курсовой работы, студент отвечает на вопросы преподавателя по теоретической и практической части курсовой работы	Отлично: обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы. Хорошо: знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. Удовлетворительно: знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности в изложении материала. Неудовлетворительно: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Экзамен	1. Основные понятия дисциплины: информация, категории доступа к информации, информация как предмет собственности, угрозы безопасности информации, формы утечки информации, объект информатизации. Основные направления технической защиты информации. 2. Технические каналы утечки информации, обрабатываемой техническими средствами. Общая характеристика, основные понятия и определения. Понятия ТСПИ, ВТСС. 3. Электромагнитные каналы утечки информации. Основные источники ПЭМИ, их характеристики. Понятия контролируемой зоны, опасной зоны 2 (зоны R2). Способы перехвата ПЭМИ ТСПИ. 4. Электрические каналы утечки информации. Линии и цепи, в которых могут возникать наводки. Понятия сосредоточенной и распределенной случайных антенн, зоны r1 (r1'). Условия перехвата наведенных сигналов. Способы

	перехвата наводок информационных сигналов. 5. Специально создаваемые технические каналы утечки информации: перехват информации способом «высокочастотного облучения». 6. Специально создаваемые технические каналы утечки информации: перехват информации с помощью закладных устройств, их классификация. 7. Типы аппаратных закладок (перехват изображений, выводимых на экран монитора; перехват информации, вводимой с клавиатуры ПЭВМ, выводимой на периферийные устройства, записываемой на жесткий диск ПЭВМ). 8. Общая характеристика речевого сигнала: понятия акустической информации, акустического сигнала, речевой информации, первичных и вторичных источников акустических сигналов, акустического поля, акустического луча, фронта волны. Линейные и энергетические характеристики акустического поля. 9. Уровни характеристик акустического поля. Интенсивность акустических колебаний. 10. Простые (тональные) и сложные акустические сигналы. Группы характеристик речи (семантические (смысловые), фонетические, физические). Частотные характеристики звуков речи, форманты и антиформанты. Речевой сигнал как процесс, развивающийся во времени и по частоте. 11. Характеристики звуковых формант как составляющих звуков речи. Октавные полосы частотного диапазона речи. Интегральный уровень акустических шумов. Понятность речевого сообщения. 12. Понятие выделенного (защищаемого) помещения. Классификация технических каналов утечки акустической (речевой) информации. 13. Прямые акустические технические каналы утечки информации: способы перехвата информации, их преимущества и недостатки. Цифровые диктофоны. 14. Типы закладных устройств для перехвата акустической информации. Проводные микрофонные системы, средства повышения разборчивости речи. Сетевые закладки. 15. Закладные устройства с передачей информации по телефонной линии. 16. Закладные устройства типа эндовибратора. 17. Закладные устройства типа аудиотранспондера. Перехват речевой информации с использованием направленных микрофонов. 18. Акустовибрационные технические каналы утечки информации. Средства, способы и оценка возможности перехвата информации. 19. Акустооптический (лазерный) технический канал утечки информации. Средства и способы перехвата информации. Повышение дальности разведки. 20. Акустоэлектрические технические каналы утечки информации. Средства и способы перехвата информации. Высокочастотное навязывание. 21. Акустоэлектромагнитные (параметрические) технические каналы утечки информации. Типы каналов, средства и способы перехвата информации. Высокочастотное облучение. 22. Технические каналы утечки информации при ее передаче по каналам связи: электрический, индукционный, за счет паразитных связей, электромагнитный. 23. Аналоговый и дискретный (цифровой) каналы связи. Способы перехвата информации, передаваемой по каналам проводной связи. 24. Способы перехвата информации, передаваемой по каналам радиосвязи: транкинговой связи, сотовой радиотелефонной связи (JSM, CDMA), системам беспроводных телефонов (аналоговым: CT-0R, CT-1R и цифровым: CT-2R, DECT). Стандарты связи, средства и способы перехвата информации. 25. Способы перехвата информации, передаваемой по каналам радиосвязи: сетям радиодоступа (WiFi, WiMax), инфракрасной связи (IrDA), Bluetooth (IEEE 802.15.1). Стандарты связи, средства и способы перехвата информации. 26. Способы скрытого видеонаблюдения и съемки. Типы перехватываемой информации. Аппаратура перехвата. 27. Классификация технических каналов утечки информации и способов перехвата информации по ним. Технические каналы утечки акустической (1),

	видовой (2) информации; информации, обрабатываемой средствами вычислительной техники, за счет ПЭМИН (3); при передаче информации по каналам связи (4). Материально-вещественные каналы утечки информации (5). Каналы утечки информации за счет несанкционированного доступа (НСД) к ПЭВМ (6). 28. Классификация технических средств разведки (ТСР) иностранных государств: принципы классификации (по принадлежности государству, по физическим принципам построения аппаратуры, по местонахождению носителей ТСР). 29. Технические средства радиоэлектронной и оптико-электронной разведки. 30. Средства фотографической, визуально-оптической разведки. Технические средства акустической, гидроакустической, магнитометрической, химической, радиационной, сейсмической разведки. Компьютерная разведка. 31. Оценка возможностей технических средств разведки по перехвату информации: обоснование критериев возможностей средств радиоразведки по перехвату информации. 32. Оценка возможностей средств радиоразведки по обнаружению сигналов и измерению их параметров. 33. Оценка возможностей средств радиоразведки по определению местоположения радиоэлектронных средств. 34. Оценка возможностей акустической речевой разведки. 35. Оценка возможностей средств оптико-электронной разведки. 36. Методы и средства защиты информации от утечек по техническим каналам: организация защиты речевой информации. Пассивные средства защиты выделенных помещений. Звукоизоляция помещений. 37. Аппаратура и способы активной защиты помещений от утечки речевой информации: линейное зашумление. Оптимальные параметры помех, особенности постановки акустических и виброакустических помех, выбор систем виброакустической защиты. 38. Аппаратура и способы активной защиты помещений от утечки речевой информации: пространственное зашумление. Подавление диктофонов, нейтрализация радиомикрофонов. 39. Пассивные способы подавления опасных электрических сигналов акустоэлектрических преобразователей: отключение источников, фильтрация, ограничение уровня опасных сигналов; применение буферных устройств. 40. Защита электросети: помехоподавляющие фильтры и разделительные трансформаторы. Защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонной линии. 41. Защита информации, обрабатываемой техническими средствами: экранирование электромагнитных полей, заземление. 42. Методы и средства защиты информации от утечек по техническим каналам: организация защиты информации от утечки, возникающей при работе вычислительной техники, за счет ПЭМИН. Характеристики канала утечки информации за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН. 43. Критерии защищенности средств вычислительной техники (СВТ). Нормированные уровни помех в каналах утечки. Основные задачи и принципы защиты СВТ. 44. Методика проведения специальных исследований технических средств электронной вычислительной техники (ЭВТ). Графический метод расчета радиуса опасной зоны 2 (зоны R2) технических средств ЭВТ. 45. Мероприятия по выявлению технических каналов утечки информации: специальные проверки (СП), специальные обследования (СО), специальные исследования (СИ). 46. Способы и средства предотвращения утечки информации по материально-вещественному каналу.

	47. Организация защиты ПЭВМ от НСД. Построение системы защиты: подсистемы управления доступом (дискреционный и мандатный принципы), регистрации и учета, контроля целостности, криптозащиты. 48. Состав типового комплекса защиты от НСД. 49. Динамика работы комплекса защиты от НСД. 50. Дополнительные механизмы защиты от несанкционированного доступа к ПЭВМ.
Выполнение и защита курсовой работы	1. Описание объекта. 2. Схема контролируемой зоны объекта и размещения защищаемого помещения. 3. Схема организационно-штатной структуры организации (предприятия). 4. Перечень сведений, подлежащих защите. 5. Структурирование защищаемой информации (ПЭМИН, речевая, видовая). 6. Схема защищаемого помещения. 7. Параметры защищаемого помещения (стены, пол, потолок, окна, двери, предметы мебели, технические средства, инженерные и технические коммуникации). 8. Угрозы (воздействия и утечки) и источники угроз (внутренние, внешние, случайные) защищаемой информации. 9. Моделирование технических каналов утечки информации (формулирование задач работы). Выбор контрольных точек, выявление слабых мест. 10. Выбор методов защиты информации (активные, пассивные). 11. Организационно-режимные меры защиты. 12. Выбор и обоснование средств защиты информации. 13. Нормативные методические документы ФСБ России и ФСТЭК России, использованные при организации защиты информации от утечек по техническим каналам.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. 1. Вестник УрФО. Безопасность в информационной сфере. — Челябинск: Изд. центр ЮУрГУ.

г) методические указания для студентов по освоению дисциплины:

1. Титульный лист курсовой работы
2. Антясов И.С. Техническая защита информации: методические указания к лабораторным работам
3. Задание на курсовую работу

из них: учебно-методическое обеспечение самостоятельной работы студента:

4. Титульный лист курсовой работы
5. Задание на курсовую работу

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Основная литература	Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Основная литература	Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
4	Методические пособия для самостоятельной работы студента	Каторин, Ю. Ф. Техническая защита информации: Лабораторный практикум / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак ; под редакцией Ю. Ф. Каторина. — Санкт-Петербург : НИУ ИТМО, 2013. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71124 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
5	Дополнительная литература	Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва : ИНТУИТ, 2016. — 424 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100275 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

6	Дополнительная литература	Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 26.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Устройство локального блокирования абонентских терминалов радиотелефонной связи «Бархан-1», Специализированный генератор «Мангуст», Переносной комплекс для измерений ПЭМИН «Навигатор П3Г» в составе: анализатор спектра NEXINS-30A с предусилителем, ПО «Навигатор» о встроенной тестовой программой «Навигатор ТЕСТ-1», комплект измерительных антенн АИ 5-0 и АИР 3-2, пробник напряжения «Шмель», штатив диэлектрический для крепления и установки антенн, Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Многофункциональный поисковый прибор ST 031 «Пиранья», Универсальный зонд-монитор для обнаружения устройств негласного съема информации «СРМ-700 Deluxe», Нелинейный локатор «Родник-2К», Детектор поля «ST-006», средство защиты информации, от утечки информации за счет побочных электромагнитных излучений и наводок «Соната – Р2», система акустической и виброакустической защиты "Соната АВ модель 1Б», система акустической и виброакустической

		защиты "Соната АВ модель 3Б», Устройство комбинированной защиты, настенные информационные стенды (3 шт.)
Лабораторные занятия	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Устройство локального блокирования абонентских терминалов радиотелефонной связи «Бархан-1», Специализированный генератор «Мангуст», Переносной комплекс для измерений ПЭМИН «Навигатор ПЗГ» в составе: анализатор спектра NEXINS-30A с предусилителем, ПО «Навигатор» о встроенной тестовой программой «Навигатор ТЕСТ-1», комплект измерительных антенн АИ 5-0 и АИР 3-2, пробник напряжения «Шмель», штатив диэлектрический для крепления и установки антенн, Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Многофункциональный поисковый прибор ST 031 «Пиранья», Универсальный зонд-монитор для обнаружения устройств негласного съема информации «СРМ-700 Deluxe», Нелинейный локатор «Родник-2К», Детектор поля «ST-006», средство защиты информации, от утечки информации за счет побочных электромагнитных излучений и наводок «Соната – Р2», система акустической и виброакустической защиты "Соната АВ модель 1Б», система акустической и виброакустической защиты "Соната АВ модель 3Б», Устройство комбинированной защиты, настенные информационные стенды (3 шт.)