

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

(Наименование института)



УТВЕРЖДАЮ:

Директор института

А.А. Галкин

« 26 » августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

(наименование дисциплины)

направление подготовки / специальность

10.05.04 «Информационно-аналитические системы безопасности»

(код и наименование направления подготовки (специальности))

направленность (профиль) подготовки

Автоматизация информационно-аналитической деятельности

(направленность (профиль) подготовки)

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита информации от утечки по техническим каналам» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности». В процессе подготовки обеспечивается формирование у студентов обобщенного представления об основных понятиях и технических средствах защиты информации. В ходе освоения дисциплины проводится ознакомление студентов с техническими каналами утечки информации, активными и пассивными методами защиты информации от утечек, средствами поиска закладок и аппаратурой несанкционированного съема информации по техническим каналам.

Задачей дисциплины «Защита информации от утечки по техническим каналам» является изучение: основ технических средств защиты информации, физических процессов формирования утечек информации по техническим каналам; технических характеристик и свойств аппаратуры защиты от утечек и поиска технических средств нелегального съема информации. Задачей дисциплины также является формирование: представлений о структуре, принципах функционирования и организации, технических характеристиках средств защиты информации; о физических основах формирования каналов утечки информации и средствах предотвращения утечек; о методах моделирования, проектирования, монтажа и настройки технических средств защиты информации. Задачей дисциплины также является овладение навыками практической деятельности в области моделирования и анализа технических средств защиты информации с использованием средств вычислительной техники, умение использовать соответствующее специализированное программное обеспечение.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части Блока Б1 (код Б1.О.06). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, практических занятий, лабораторных работ и самостоятельной работы. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
ОПК-4 Способен применять физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1.1	Знать основные понятия, законы и модели электричества и магнетизма применительно к техническим средствам ЗИ	Тестовые вопросы, КР
	ОПК-4.1.2	Знать основные понятия, законы и модели теории колебаний и волн, оптики, физики твердого тела, статистической физики и термодинамики применительно к техническим средствам ЗИ	
	ОПК-4.1.3	Знать особенности физических эффектов и явлений, используемых для обеспечения	

		информационной безопасности
ОПК-4.1.4		Знать технические средства контроля эффективности мер защиты информации
ОПК-4.1.5		Знать принципы построения средств защиты информации от «утечки» по техническим каналам
ОПК-4.1.6		Знать технические каналы «утечки» информации
ОПК-4.1.7		Знать организацию защиты информации от «утечки» по техническим каналам на объектах информатизации
ОПК-4.1.8		Знать классификацию и количественные характеристики технических каналов утечки информации
ОПК-4.1.9		Знать технические характеристики и возможности аппаратуры защиты информации от утечки по техническим каналам и аппаратуры средств несанкционированного съема информации по техническим каналам
ОПК-4.2.1		Уметь анализировать и оценивать угрозы утечки информации по техническим каналам на объекте информатизации
ОПК-4.2.2		Уметь формировать комплекс мер по технической защите объекта информатизации от утечки информации по техническим каналам с учетом технической обоснованности и реализуемости
ОПК-4.2.3		Уметь использовать физические модели и законы в постановке и решении прикладных задач в профессиональной деятельности
ОПК-4.2.4		Уметь контролировать безотказное функционирование технических средств защиты информации
ОПК-4.2.5		Уметь восстанавливать (заменять) отказавшие технические средства защиты информации
ОПК-4.3.1		Владеть навыками выявления основных угроз безопасности информации в автоматизированных системах
ОПК-4.3.2		Владеть навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ОПК-4.3.3		Владеть методами и средствами технической защиты информации
ОПК-4.3.4		Владеть методами расчета и инструментального контроля показателей технической защиты информации

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов

**Тематический план
форма обучения – очная**

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	в форме практической подготовки		
1	Радиочастотомеры и интерсептеры.	7	1	2	2			1	
2	ПАК радиоконтроля. Радиопеленгаторы	7	2	2	2	4		2	
3	Средства видовой разведки. Средства ТВ наблюдения.	7	3	2	2			1	
4	Средства обнаружения видеокамер.	7	4	2	2	4		2	
5	Каналы утечки по линиям связи. Характеристики пров. линий связи.	7	5	2	2			1	
6	Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы.	7	6	2	2	4		2	Рейтинг-контроль №1
7	Средства защиты моб. связи и wi-fi	7	7	2	2			1	
8	Акустические и виброакустические каналы. Разборчивость акустической информации.	7	8	2	2	4		2	
9	Магнитные и электромагнитные каналы. ПЭМИН.	7	9	2	2			1	
10	Методы и средства акустической и виброакустической защиты объекта.	7	10	2	2	4		2	
11	Методика акустической и виброакустич. защиты помещения. Генераторы шума	7	11	2	2			1	
12	Противодействие электронным устройствам перехвата информации.	7	12	2	2	4		2	Рейтинг-контроль №2
13	Исследование ПЭМИН электронной техники и средств обработки информации.	7	13	2	2			1	
14	Средства фильтрации сигналов.	7	14	2	2	4		2	
15	Методы и средства экранирования	7	15	2	2			1	
16	Нелинейные локаторы. Методика поиска закладных устройств.	7	16	2	2	4		2	
17	Специальные проверки и специальные обследования помещений.	7	17	2	2			1	
18	Аттестация объектов информатизации	7	18	2	2	4		2	Рейтинг-контроль №3
Всего за 7 семестр:		180		36	36	36		27	Экзамен (45)
Наличие в дисциплине КП/КР		ДА							
Итого по дисциплине		180		36	36	36		27	Экзамен (45) Курсовая работа

Содержание лекционных занятий по дисциплине

Тема 1. Радиочастотомеры и интерсептеры. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 2. Программно-аппаратные комплексы радиоконтроля. Радиопеленгаторы. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 3. Средства видовой разведки. Средства ТВ наблюдения. Средства фоторазведки. Фотокамеры. Закамуфлированные средства. Средства телевизионного наблюдения. Бинокли, монокуляры, подзорные трубы. Приборы ночного видения. Инфракрасные прожекторы. Портативные видеокамеры.

Тема 4. Средства обнаружения видеокамер. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 5. Каналы утечки по линиям связи. Характеристики проводных линий связи. Основные термины, определения и технические характеристики средств защиты информации в проводных линиях связи. Основные способы защиты телефонных линий.

Тема 6. Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 7. Средства защиты мобильной связи и wi-fi. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 8. Акустические и виброакустические каналы. Разборчивость акустической информации. Методики расчетов возможности утечки информации по акустическому каналу.

Тема 9. Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки. Виды акустоэлектрических преобразований. Паразитные излучения и наводки. Классификация акустических радиопередающих закладных устройств. Методы ВЧ навязывания. Технические характеристики и термины радиоприемной аппаратуры.

Тема 10. Методы и средства акустической и виброакустической защиты объекта. Пространственное и линейное зашумление. Пассивные методы защиты речевой информации. Активные методы защиты речевой информации. Определение соответствия помещения требованиям выделенного помещения. Технические средства защиты.

Тема 11. Методика акустической и виброакустич. защиты помещения. Генераторы шума. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 12. Противодействие электронным устройствам перехвата информации.

Тема 13. Исследование ПЭМИН электронной техники и средств обработки информации. Принципы действия, технические характеристики, особенности эксплуатации технических средств активной защиты от ПЭМИН.

Тема 14. Средства фильтрации сигналов. Типы фильтров, их технические характеристики способы применения и особенности эксплуатации.

Тема 15. Методы и средства экранирования. Основные термины, определения и технические характеристики средств защиты информации при утечке информации по электрической сети и цепям заземления. Виды заземления, типы и свойства экранирования. Развязывание информационных сигналов. Фильтрация сигналов. Разделительные трансформаторы. Свойства и характеристики фильтров. Проходные конденсаторы в фильтрах

Тема 16. Нелинейные локаторы. Методика поиска закладных устройств. Принципы действия, технические характеристики, особенности эксплуатации.

Тема 17. Специальные проверки и специальные обследования помещений.

Тема 18. Аттестация объектов информатизации. Назначение, порядок проведения, типы и методы проведения измерений.

Содержание лабораторных занятий по дисциплине

- Лабораторная работа 1.** Исследование радиоэлектронного канала утечки информации;
- Лабораторные работы 2-3.** Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;
- Лабораторные работы 4-5.** Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;
- Лабораторные работы 6-7.** Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки за счет электроакустических преобразований в ТСПИ с помощью программно-аппаратного комплекса «Спрут-мини-А»;
- Лабораторная работа 8.** Исследование методики защиты телефонных линий в помещении с помощью прибора проверки проводных линий «ULAN»;
- Лабораторная работа 9.** Исследование методики защиты телефонных линий в помещении с помощью прибора защиты телефонных переговоров «Прокруст 2000».

Содержание практических занятий по дисциплине

- Тема 1.** Средства обнаружения видеокамер.
- Тема 2.** Каналы утечки по линиям связи. Характеристики проводных линий связи.
- Тема 3.** Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы.
- Тема 4.** Разборчивость акустической информации.
- Тема 5.** Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки.
- Тема 6.** Методы и средства акустической и виброакустической защиты объекта.
- Тема 7.** Методика акустической и виброакустич. защиты помещения. Генераторы шума
- Тема 8.** Исследование ПЭМИН электронной техники и средств обработки информации.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Перечень вопросов к рейтинг-контролю №1

1. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
2. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
3. Чем обусловлены материально-вещественные каналы утечки информации?
4. Основные технические характеристики микрофонов.
5. Физические основы явления реверберации звука.
6. Технические средства акустической и виброакустической защиты выделенного помещения.
7. Основные характеристики и принцип действия параболического микрофона.
8. Основные характеристики и принцип действия лазерных микрофонов.
9. Классификация акустических закладок.
10. Принцип действия полуактивных радиозакладок.
11. Классификация телефонных закладок.
12. Физический принцип действия бесконтактных телефонных закладок.
13. Назначение и основные технические характеристики сканерных приемников.
14. Основные типы организации сканирования радиочастот.
15. Назначение и основные технические характеристики анализаторов спектра.

16. Назначение и основные технические характеристики радиочастотомеров.
17. Назначение и основные технические характеристики интерсепторов.
18. Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.

Перечень вопросов к рейтинг-контролю №2

1. Основные характеристики радиопеленгаторов.
2. Основные характеристики антенно-фидерных устройств.
3. Технические средства контроля сотовой связи.
4. Технические характеристики средств фоторазведки.
5. Основные технические характеристики средств видеонаблюдения.
6. Системы слежения (наблюдения) за перемещением транспортных средств.
7. Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
8. Классификация методов и средств поиска электронных устройств перехвата информации
9. Электростатическое экранирование технических средств
10. Магнитостатическое экранирование технических средств
11. Электромагнитное экранирование технических средств
12. Заземление технических средств
13. Электростатическое экранирование технических средств
14. Магнитостатическое экранирование технических средств
15. Электромагнитное экранирование технических средств
16. Заземление технических средств
17. Развязывание информационных сигналов
18. Фильтрация информационных сигналов
19. Пространственное зашумление
20. Линейное зашумление

Перечень вопросов к рейтинг-контролю №3

1. Пассивные методы защиты акустической (речевой) информации
2. Активные методы защиты акустической (речевой) информации
3. Характеристики и способы повышения звукоизоляции помещений
4. Виброакустическая маскировка
5. Методы и средства обнаружения и подавления диктофонов и акустических закладок.
6. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи
7. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения
8. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи
9. Защита телефонных линий компенсационным методом и методом "выжигания"
10. Специальная проверка и спецобследование помещений
11. Нелинейные локаторы. Методика поиска закладных устройств.
12. Специальные проверки и специальные обследования помещений.
13. Аттестация объектов информатизации

5.2. Промежуточная аттестация

Примерный перечень вопросов к экзамену

1. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
2. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
3. Чем обусловлены материально-вещественные каналы утечки информации?
4. Основные технические характеристики микрофонов.

5. Физические основы явления реверберации звука.
6. Технические средства акустической и виброакустической защиты выделенного помещения.
7. Основные характеристики и принцип действия параболического микрофона.
8. Основные характеристики и принцип действия лазерных микрофонов.
9. Классификация акустических закладок.
10. Принцип действия полуактивных радиозакладок.
11. Классификация телефонных закладок.
12. Физический принцип действия бесконтактных телефонных закладок.
13. Назначение и основные технические характеристики сканерных приемников.
14. Основные типы организации сканирования радиочастот.
15. Назначение и основные технические характеристики анализаторов спектра.
16. Назначение и основные технические характеристики радиочастотомеров.
17. Назначение и основные технические характеристики интерсепторов.
18. Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.
19. Основные характеристики радиопеленгаторов.
20. Основные характеристики антенно-фидерных устройств.
21. Технические средства контроля сотовой связи.
22. Технические характеристики средств фоторазведки.
23. Основные технические характеристики средств видеонаблюдения.
24. Системы слежения (наблюдения) за перемещением транспортных средств.
25. Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
26. Классификация методов и средств поиска электронных устройств перехвата информации
27. Электростатическое экранирование технических средств
28. Магнитостатическое экранирование технических средств
29. Электромагнитное экранирование технических средств
30. Заземление технических средств
31. Электростатическое экранирование технических средств
32. Магнитостатическое экранирование технических средств
33. Электромагнитное экранирование технических средств
34. Заземление технических средств
35. Развязывание информационных сигналов
36. Фильтрация информационных сигналов
37. Пространственное зашумление
38. Линейное зашумление
39. Пассивные методы защиты акустической (речевой) информации
40. Активные методы защиты акустической (речевой) информации
41. Характеристики и способы повышения звукоизоляции помещений
42. Виброакустическая маскировка
43. Методы и средства обнаружения и подавления диктофонов и акустических закладок.
44. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи
45. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения
46. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи
47. Защита телефонных линий компенсационным методом и методом "выжигания"
48. Специальная проверка и спецобследование помещений
49. Нелинейные локаторы. Методика поиска закладных устройств.
50. Специальные проверки и специальные обследования помещений.
51. Аттестация объектов информатизации

5.3. Самостоятельная работа обучающегося.

Примерные темы курсовой работы 7 семестр

Тема работы: «Моделирование технических каналов утечки информации на объекте, создание инженерно-технической защиты от НСД» по вариантам. Всего в методических рекомендациях по выполнению курсовой работы имеется 18 вариантов заданий.

Вопросы для выполнения в курсовой работе:

- Провести расстановку в защищаемом помещении мебели, ТСПИ, ОТСС и ВТСС;
- Скорректировать генплан территориального размещения объекта на местности;
- Структурирование информации на объекте, создание основных характеристик объекта защиты;
- Формирование путей физического проникновения злоумышленников на объект;
- Классификация возможных каналов утечки информации на объекте;
- Формирование модели получения информации по техническим каналам с объекта защиты;
- Расчет уровней акустического сигнала на строительных конструкциях;
- Выбор и описание тактико-технических характеристик устройств съема информации;
- Формирование модели защиты информации от утечки по техническим каналам с объекта защиты;
- Выбор и описание тактико-технических характеристик средств защиты информации;
- Изучить организацию и проведение обследований объектов на предмет состояния инженерно-технического укрепления, составление акта обследования состояния инженерно-технического укрепления объекта;
- Проектирование охранно-тревожной сигнализации объектов на основе оборудования ИСБ «Орион» НВП «Болид». На основании Р78.36.031-2013, изученного лекционного материала и примера составления проектной документации (выданного в электронном виде) составить по имеющимся вариантам (16шт) планировок:
 - структурную схему;
 - поэтажные планы сетей охранно-тревожной сигнализации (ОТС);
 - пояснительную записку;
 - расчет емкости резервного питания;
- спецификацию оборудования.

Примерные вопросы и задания для самостоятельной работы студентов 7 семестр

- Средства фильтрации сигналов. Методы и средства экранирования.
- Нелинейные локаторы. Методика поиска закладных устройств.
- Специальные проверки и специальные обследования помещений.
- Аттестация объектов информатизации
- Инженерно-техническое укрепление объектов
- Извещатели охранной сигнализации. Основные ТТД, правила установки и эксплуатации
- Организация централизованной охраны объектов. Системы передачи извещений
- Интегрированные системы и комплексы технических средств охраны и безопасности
- Организация эксплуатационно-технического обслуживания технических средств охраны и безопасности
- Основные понятия СКУД
- Методы и средства идентификации в СКУД
- Устройства преграждающие управляемые СКУД
- Основные термины, понятия и определения СВН
- Устройства управления и передачи видео изображений. Устройства регистрации видеоизображений

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
1. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - Москва :Гор. линия-Телеком, 2015. - 586 с. ISBN 978-5-9912-0424-8	2015	https://znanium.com/catalog/product/895240
2. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Рагозин Ю. Н. - Санкт-петербург : ИЦ Интермедия, 2019. - 216 с. - ISBN 978-5-4383-0182-0	2019	https://www.studentlibrary.ru/book/ISBN9785438301820.html
3. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики : учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2018. – 161 с. (Комплексная защита объектов информатизации. Кн. 26). – ISBN 978-5-9984-0875-5, №госрегистрации №0321803506	2018	http://dspace.www1.vlsu.ru/bitstream/123456789/7165/1/00792.pdf
4. Тельный А. В., Монахов Ю.М. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Аппаратура поиска каналов и устройств несанкционированного съема информации. Методики и рекомендации по применению технических средств защиты информации: учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2018. 86 с. – (Комплексная защита объектов информатизации. Кн. 27). – ISBN 978-5-9984-0874-8, № госрегистрации № 0321803507.	2018	http://dspace.www1.vlsu.ru/bitstream/123456789/7185/1/00793.pdf
5. Тельный А. В. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Проектирование технических средств защиты территорий и объектов от несанкционированного доступа: учеб. пособие / А. В. Тельный; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 251 с. – (Комплексная защита объектов информатизации. Кн. 29). – ISBN 978-5-9984-1172-4	2020	http://dspace.www1.vlsu.ru/bitstream/123456789/8947/1/02160.pdf
Дополнительная литература		
1. Сагдеев, К. М. Физические основы защиты информации : учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 394 с. : 387-388	2021	https://biblioclub.ru/index.php?page=book&id=458285
2. Ишейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.	2021	https://znanium.com/catalog/product/1178151

Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6.		
3. Рагозин, Ю. Н. Инженерно-техническая защита информации / Рагозин Ю. Н. - Санкт-петербург : ИЦ Интермедия, 2018. - 168 с. - ISBN 978-5-4383-0161-5.	2018	https://www.studentlibrary.ru/book/ISBN9785438301615.html

6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: <http://inside-zi.ru/pages/about.html>
2. Электронный журнал «Спецтехника и Связь», Режим доступа: <http://www.st-s.ru/>
3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: <http://sccs.intelgr.com/>
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: <http://www.ess.ru/>
5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: <http://asbgroup.ru/izdaniya/zhurnal-bdi/>

6.3. Интернет-ресурсы

1. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: <http://spymarket.com/>
2. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: <http://www.mascom.ru/> (дата обращения: 13.06.2018).
3. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: <https://www.nelk.ru/>
4. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: <http://www.sinf.ru/>
5. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: <http://www.profinfo.ru/>
6. Сайт компании «Сюртель» г. Москва [Электронный ресурс] // URL: <http://www.suritel.ru/>
7. ЗАО ПФ «Элвира» Московская обл. г. Железнодорожный [Электронный ресурс] // URL: <http://www.elvira.ru/>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор

ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3», учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Chaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил _____ доцент кафедры ИЗИ Тельный А.В.
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) _____ Заместитель руководителя РАЦ ООО
«ИнфоЦентр» _____ к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры _____ ИЗИ
Протокол № _____ от _____ года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № _____ от _____ года
Председатель комиссии д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, должность, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год
Протокол заседания кафедры № 14 от 28.06.22 года
Заведующий кафедрой _____ д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20 ____ / 20 ____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____ /М.Ю. Монахов/

Рабочая программа одобрена на 20 ____ / 20 ____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____ /М.Ю. Монахов/

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
в рабочую программу дисциплины
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
образовательной программы специальности
10.05.04 «Информационно-аналитические системы безопасности»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____ / _____

Подпись

ФИО