

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)



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

(наименование дисциплины)

Направление 10.03.01 "Информационная безопасность"

Направленность "Комплексная защита объектов информатизации"

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	3/108	36		18	54	Зачет
6	5/180	36		36	63	Экзамен (45ч)
7	6/216	36		36	108	Экзамен (36ч), КР
Итого	14/504	108		90	225	Экзамен (81ч), КР

Владимир 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Техническая защита информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование у студентов обобщенного представления об основных понятиях и технических средствах защиты информации. Ознакомление студентов с техническими каналами утечки информации, активными и пассивными методами предотвращения утечек информации, средствами поиска закладок и аппаратурой съема информации по техническим каналам.

Задачей дисциплины «Техническая защита информации» является изучение:

- основ технических средств защиты информации, изучение формирования утечек информации по техническим каналам, аппаратуры защиты от утечек и поиска технических средств нелегального съема информации.

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.

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 ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к обязательным дисциплинам вариативной части Блока Б1 (код Б1.Б.15). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на третьем и четвертом курсе в 5, 6 и 7 семестрах, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Физические процессы в информационной безопасности», «Теория информации», «Электроника и схемотехника» профессионального цикла по направлению 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Физика».

Курс тесно взаимосвязан с другими дисциплинами.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-3 – способностью администрировать подсистемы информационной безопасности объекта защиты

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

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

ПК-12 - способностью принимать участие в проведении экспериментальных исследований системы защиты информации

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом,

охранного телевидения; - 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; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - современные компьютерные технологии и программное обеспечение для решения задач, связанных с процедурами обработки аналитической информации и поиском информации (ПК-3; ПК-5 ПК-6; ПК-12);

2) Уметь: - анализировать и формализовать задачи своей профессиональной деятельности (научно-исследовательские, экспертно-аналитические, организационно-управленческие и др.) и выбирать адекватные пути и методы для их решения; квалифицированно применять полученные знания; - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости; - осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-3; ПК-5 ПК-6; ПК-12).

3) Владеть: -методами и средствами выявления угроз безопасности автоматизированным системам; - навыками организации и обеспечения режима секретности; - методами технической защиты информации; - методами формирования требований по защите информации; -методами расчета и инструментального контроля показателей технической защиты информации; - профессиональной терминологией; -навыками безопасного использования технических средств в профессиональной деятельности; - навыками поиска технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов в профессиональной деятельности; - квалифицированно использовать сетевые ресурсы с целью организации интерактивного взаимодействия, а также поиска и передачи информации в локальных и глобальных информационных сетях (ПК-3; ПК-5 ПК-6; ПК-12).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность проектировать систему инженерно-технической защиты объекта информатизации от несанкционированного доступа и проектировать систему защиты помещений от утечки информации по техническим каналам

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 14 зачетных единиц, 504 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1	Основные положения и теоретические основы инженерно-технической защиты информации.	5	1-2	4		2		6		4(66%)	
2	Средства и методы инженерно-технической защиты информации.	5	3-4	4		2		6		4(66%)	
3	Демаскирующие признаки объектов защиты.	5	5-6	4		2		6		4(66%)	Рейтинг-контроль №1
4	Основные демаскирующие признаки, характеризующие физические свойства сигналов.	5	7-8	4		2		6		4(66%)	
5	Основные свойства информации как предмета инженерно-технической защиты.	5	9-10	4		2		6		4(66%)	
6	Органы добывания информации. Роль разведки в деятельности государств и коммерческих структур.	5	11-12	4		2		6		4(66%)	Рейтинг-контроль №2
7	Оптические каналы утечки информации.	5	13-14	4		2		6		4(66%)	
8	Радиоэлектронные каналы утечки информации.	5	15-16	4		2		6		4(66%)	
9	Акустические каналы утечки информации.	5	17-18	4		2		6		4(66%)	Рейтинг-контроль №3
Всего по 5 семестру:				36		18		54		36(66%)	Зачет
10	Составные акустоэлектрон. и акустооптические каналы утечки информации.	6	1-2	4		4		7		4(50%)	
11	Материально-вещественные каналы утечки информации	6	3-4	4		4		7		4(50%)	
12	Классификация методов и средств защиты информации от утечки по техническим каналам.	6	5-6	4		4		7		4(50%)	Рейтинг-контроль №1
13	Технические средства акустической разведки. Принципы функционирования и основные характеристики микрофонов	6	7-8	4		4		7		4(50%)	
14	Направленные микрофоны. Параболические и лазерные микрофоны. Микрофон- труба.	6	9-10	4		4		7		4(50%)	
15	Виды и типы акустических закладок	6	11-12	4		4		7		4(50%)	Рейтинг-контроль №2
16	Полуактивные закладки	6	13-14	4		4		7		4(50%)	
17	Средства радио-и РТ разведки и поисковые средства.	6	15-16	4		4		7		4(50%)	
18	Сканерные приемники. Анализаторы спектра.	6	17-18	4		4		7		4(50%)	Рейтинг-контроль №3
Всего по 6 семестру:				36		36		63		36(50%)	ЭКЗАМЕН

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
19	Радиочастотомеры и интерсептеры.	7	1	2		2		6		2(50%)	
20	ПАК радиоконтроля. Радиопеленгаторы	7	2	2		2		6		2(50%)	
21	Средства видовой разведки. Средства ТВ наблюдения.	7	3	2		2		6		2(50%)	
22	Средства обнаружения видеокамер.	7	4	2		2		6		2(50%)	
23	Каналы утечки по линиям связи. Характеристики проводных линий связи.	7	5	2		2		6		2(50%)	
24	Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы.	7	6	2		2		6		2(50%)	Рейтинг-контроль №1
25	Средства защиты мобильной связи и wi-fi	7	7	2		2		6		2(50%)	
26	Акустические и виброакустические каналы. Разборчивость акустической информации.	7	8	2		2		6		2(50%)	
27	Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки.	7	9	2		2		6		2(50%)	
28	Методы и средства акустической и виброакустической защиты объекта.	7	10	2		2		6		2(50%)	
29	Методика акустической и виброакустич. защиты помещения. Генераторы шума	7	11	2		2		6		2(50%)	
30	Противодействие электронным устройствам перехвата информации.	7	12	2		2		6		2(50%)	Рейтинг-контроль №2
31	Исследование ПЭМИН электронной техники и средств обработки информации.	7	13	2		2		6		2(50%)	
32	Средства фильтрации сигналов.	7	14	2		2		6		2(50%)	
33	Методы и средства экранирования.	7	15	2		2		6		2(50%)	
34	Нелинейные локаторы. Методика поиска закладных устройств.	7	16	2		2		6		2(50%)	
35	Специальные проверки и специальные обследования помещений.	7	17	2		2		6		2(50%)	
36	Аттестация объектов информатизации	7	18	2		2		6		2(50%)	Рейтинг-контроль №3
Всего по 7 семестру:				36		36		108	КР	36(50%)	Экзамен
ИТОГО:				108		90		225		108/ 54%	Зачет, Экзамен, ЭКЗАМЕН

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению 10.03.01 «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП направления 10.03.01 «Информационная безопасность», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

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

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1 семестр 5

- Перечислите цели защиты информации.
- Перечислите задачи ИТЗИ.
- Какие признаки объекта защиты называют демаскирующими?
- Приведите классификацию демаскирующих признаков объекта защиты.
- Охарактеризуйте видовые демаскирующие признаки.
- Охарактеризуйте демаскирующие признаки сигналов.
- Дайте классификацию сигналов.
- Охарактеризуйте демаскирующие признаки веществ.
- Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?

- Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?
- Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?

Вопросы рейтинг-контроля №2 семестр 5

- Перечислите свойства информации как предмета инженерно-технической защиты.
- Понятие шумоподобных сигналов.
- Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?
- Какие типы и виды помех в каналах связи Вы знаете?
- Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.
- Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?
- Перечислите основные источники функциональных сигналов.
- Проведите классификацию источников опасных сигналов по их физическому происхождению.
- Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
- Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
- Типы угроз, создаваемых акустоэлектрическими преобразователями.
- Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.

Вопросы рейтинг-контроля №3 семестр 5

- Типы угроз, создаваемых акустоэлектрическими преобразователями.
- Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
- Назовите типы паразитных связей в радиоэлектронных средствах и физические причины их возникновения.
- Физические основы паразитных емкостных и индуктивных наводок в радиоэлектронных средствах.
- Классификация технической разведки по способам добывания информации.
- Классификация технической разведки по физической природе носителя информации.
- Основные задачи органов коммерческой разведки.
- Перечислите основные способы ведения разведки.
- Перечислите основные этапы добывания информации при разведке.
- Основные методы анализа и синтеза разведывательной информации.
- Способы доступа к разведывательной информации.
- Классификация наземных технических средств дистанционного добывания информации.
- Классификация каналов утечки информации.
- Структурная схема, физическая сущность и основные свойства оптического канала утечки информации.

Перечень вопросов к зачету 5 семестра (промежуточной аттестации по итогам освоения дисциплины):

- Перечислите цели защиты информации.
- Перечислите задачи ИТЗИ.
- Какие признаки объекта защиты называют демаскирующими?
- Приведите классификацию демаскирующих признаков объекта защиты.

- Охарактеризуйте видовые демаскирующие признаки.
- Охарактеризуйте демаскирующие признаки сигналов.
- Дайте классификацию сигналов.
- Охарактеризуйте демаскирующие признаки веществ.
- Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?
- Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?
- Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?
- Перечислите свойства информации как предмета инженерно-технической защиты.
- Понятие шумоподобных сигналов.
- Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?
- Какие типы и виды помех в каналах связи Вы знаете?
- Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.
- Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?
- Перечислите основные источники функциональных сигналов.
- Проведите классификацию источников опасных сигналов по их физическому происхождению.
- Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
- Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
- Типы угроз, создаваемых акустоэлектрическими преобразователями.
- Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
- Типы угроз, создаваемых акустоэлектрическими преобразователями.
- Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
- Назовите типы паразитных связей в радиоэлектронных средствах и физические причины их возникновения.
- Физические основы паразитных емкостных и индуктивных наводок в радиоэлектронных средствах.
- Классификация технической разведки по способам добывания информации.
- Классификация технической разведки по физической природе носителя информации.
- Основные задачи органов коммерческой разведки.
- Перечислите основные способы ведения разведки.
- Перечислите основные этапы добывания информации при разведке.
- Основные методы анализа и синтеза разведывательной информации.
- Способы доступа к разведывательной информации.
- Классификация наземных технических средств дистанционного добывания информации.
- Классификация каналов утечки информации.
- Структурная схема, физическая сущность и основные свойства оптического канала утечки информации.

Вопросы рейтинг-контроля №1 семестр 6

- Основные свойства акустического канала утечки информации.

- Основные свойства радиоэлектронного канала утечки информации.
- Основные свойства материально-вещественного канала утечки информации.
- Основные свойства акустооптического канала утечки информации.
- Основные свойства акусто-вибрационного канала утечки информации.
- Структурная схема и физическая сущность акусто-радиоэлектронного канала утечки информации.
- Комплексирование каналов утечки информации.
- Назовите основные этапы проектирования систем инженерно-технической защиты информации.
- Назовите основные типы моделирования систем инженерно-технической защиты информации.

Вопросы рейтинг-контроля №2 семестр 6

- Комплексирование каналов утечки информации.
- Назовите основные этапы проектирования систем инженерно-технической защиты информации.
- Назовите основные типы моделирования систем инженерно-технической защиты информации.
- Что включает в себя моделирование угроз информации (приведите примеры)?
- Типы контроля эффективности инженерно-технической защиты информации.
- Что включают в себя организационные меры контроля эффективности инженерно-технической защиты информации?
- Что включают в себя технические меры контроля эффективности инженерно-технической защиты информации?
- В чем отличие основных от вспомогательных технических средств и систем?
- Дайте определение контролируемой зоны.

Вопросы рейтинг-контроля №3 семестр 6

- Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
- Покажите, на каких физических процессах ОТСС и ВТСС построены основные виды каналов утечки с информационных носителей.
- Объясните физическую сущность возникновения побочных электромагнитных излучений.
- Какие причины приводят к возникновению электрических каналов утечки информации?
- Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.
- Как создаются составные каналы утечки информации?
- Приведите структуру комплекса средств перехвата радиосигналов.
- Как реализуется метод «высокочастотного навязывания»?
- Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
- Каким параметром определяется зона возможного перехвата информации?
- Каковы основные акустические параметры речевых сигналов?
- От чего зависит звукоизоляция основных строительных конструкций?

Перечень вопросов к экзамену 6 семестра (промежуточной аттестации по итогам освоения дисциплины):

- Перечислите цели защиты информации.
- Перечислите задачи ИТЗИ.
- Какие признаки объекта защиты называют демаскирующими?
- Приведите классификацию демаскирующих признаков объекта защиты.
- Охарактеризуйте видовые демаскирующие признаки.
- Охарактеризуйте демаскирующие признаки сигналов.
- Дайте классификацию сигналов.

- Охарактеризуйте демаскирующие признаки веществ.
- Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?
- Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?
- Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?
- Перечислите свойства информации как предмета инженерно-технической защиты.
- Понятие шумоподобных сигналов.
- Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?
- Какие типы и виды помех в каналах связи Вы знаете?
- Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.
- Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?
- Перечислите основные источники функциональных сигналов.
- Проведите классификацию источников опасных сигналов по их физическому происхождению.
- Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
- Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
- Типы угроз, создаваемых акустоэлектрическими преобразователями.
- Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
- Назовите типы паразитных связей в радиоэлектронных средствах и физические причины их возникновения.
- Физические основы паразитных емкостных и индуктивных наводок в радиоэлектронных средствах.
- Классификация технической разведки по способам добывания информации.
- Классификация технической разведки по физической природе носителя информации.
- Основные задачи органов коммерческой разведки.
- Перечислите основные способы ведения разведки.
- Перечислите основные этапы добывания информации при разведке.
- Основные методы анализа и синтеза разведывательной информации.
- Способы доступа к разведывательной информации.
- Классификация наземных технических средств дистанционного добывания информации.
- Классификация каналов утечки информации.
- Структурная схема, физическая сущность и основные свойства оптического канала утечки информации.
- Основные свойства акустического канала утечки информации.
- Основные свойства радиоэлектронного канала утечки информации.
- Основные свойства материально-вещественного канала утечки информации.
- Основные свойства акустооптического канала утечки информации.
- Основные свойства акусто-вибрационного канала утечки информации.
- Структурная схема и физическая сущность акусто-радиоэлектронного канала утечки информации.
- Комплексование каналов утечки информации.
- Назовите основные этапы проектирования систем инженерно-технической защиты информации.

- Назовите основные типы моделирования систем инженерно-технической защиты информации.
- Что включает в себя моделирование угроз информации (приведите примеры)?
- Типы контроля эффективности инженерно-технической защиты информации.
- Что включают в себя организационные меры контроля эффективности инженерно-технической защиты информации?
- Что включают в себя технические меры контроля эффективности инженерно-технической защиты информации?
- В чем отличие основных от вспомогательных технических средств и систем?
- Дайте определение контролируемой зоны.
- Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
- Покажите, на каких физических процессах ОТСС и ВТСС построены основные виды каналов утечки с информационных носителей.
- Объясните физическую сущность возникновения побочных электромагнитных излучений.
- Какие причины приводят к возникновению электрических каналов утечки информации?
- Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.
- Как создаются составные каналы утечки информации?
- Приведите структуру комплекса средств перехвата радиосигналов.
- Как реализуется метод «высокочастотного навязывания»?
- Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
- Каким параметром определяется зона возможного перехвата информации?
- Каковы основные акустические параметры речевых сигналов?
- От чего зависит звукоизоляция основных строительных конструкций?

Вопросы рейтинг-контроля №1 семестр 7

- Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
- Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
- Чем обусловлены материально-вещественные каналы утечки информации?
- Основные технические характеристики микрофонов.
- Физические основы явления реверберации звука.
- Технические средства акустической и виброакустической защиты выделенного помещения.
- Основные характеристики и принцип действия параболического микрофона.
- Основные характеристики и принцип действия лазерных микрофонов.
- Классификация акустических закладок.
- Принцип действия полуактивных радиозакладок.
- Классификация телефонных закладок.
- Физический принцип действия бесконтактных телефонных закладок.
- Назначение и основные технические характеристики сканерных приемников.
- Основные типы организации сканирования радиочастот.
- Назначение и основные технические характеристики анализаторов спектра.
- Назначение и основные технические характеристики радиочастотомеров.
- Назначение и основные технические характеристики интерсепторов.
- Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.

Вопросы рейтинг-контроля №2 семестр 7

- Основные характеристики радиопеленгаторов.
- Основные характеристики антенно-фидерных устройств.

- Технические средства контроля сотовой связи.
- Технические характеристики средств фоторазведки.
- Основные технические характеристики средств видеонаблюдения.
- Системы слежения (наблюдения) за перемещением транспортных средств.
- Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
- Классификация методов и средств поиска электронных устройств перехвата информации
- Электростатическое экранирование технических средств
- Магнитостатическое экранирование технических средств
- Электромагнитное экранирование технических средств
- Заземление технических средств
- Электростатическое экранирование технических средств
- Магнитостатическое экранирование технических средств
- Электромагнитное экранирование технических средств
- Заземление технических средств
- Развязывание информационных сигналов
- Фильтрация информационных сигналов
- Пространственное зашумление
- Линейное зашумление

Вопросы рейтинг-контроля №3 семестр 7

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

Перечень вопросов к экзамену 7 семестра (промежуточной аттестации по итогам освоения дисциплины):

- Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
- Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
- Чем обусловлены материально-вещественные каналы утечки информации?
- Основные технические характеристики микрофонов.
- Физические основы явления реверберации звука.
- Технические средства акустической и виброакустической защиты выделенного помещения.
- Основные характеристики и принцип действия параболического микрофона.
- Основные характеристики и принцип действия лазерных микрофонов.
- Классификация акустических закладок.
- Принцип действия полуактивных радиозакладок.

- Классификация телефонных закладок.
- Физический принцип действия бесконтактных телефонных закладок.
- Назначение и основные технические характеристики сканерных приемников.
- Основные типы организации сканирования радиочастот.
- Назначение и основные технические характеристики анализаторов спектра.
- Назначение и основные технические характеристики радиочастотомеров.
- Назначение и основные технические характеристики интерсепторов.
- Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.
- Основные характеристики радиопеленгаторов.
- Основные характеристики антенно-фидерных устройств.
- Технические средства контроля сотовой связи.
- Технические характеристики средств фоторазведки.
- Основные технические характеристики средств видеонаблюдения.
- Системы слежения (наблюдения) за перемещением транспортных средств.
- Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
- Классификация методов и средств поиска электронных устройств перехвата информации
- Электростатическое экранирование технических средств
- Магнитостатическое экранирование технических средств
- Электромагнитное экранирование технических средств
- Заземление технических средств
- Развязывание информационных сигналов
- Фильтрация информационных сигналов
- Пространственное зашумление
- Линейное зашумление
- Пассивные методы защиты акустической (речевой) информации
- Активные методы защиты акустической (речевой) информации
- Характеристики и способы повышения звукоизоляции помещений
- Виброакустическая маскировка
- Методы и средства обнаружения и подавления диктофонов и акустических закладок.
- Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи
- Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения
- Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи
- Защита телефонных линий компенсационным методом и методом "выжигания"
- Специальная проверка и спецобследование помещений
- Нелинейные локаторы. Методика поиска закладных устройств.
- Специальные проверки и специальные обследования помещений.
- Аттестация объектов информатизации

Темы лабораторных работ 5 семестр:

Лабораторная работа №1. Исследование методики защиты проводных линий связи с помощью поискового прибора ST 031P «Пиранья»;

Лабораторная работа №2. Исследование методики защиты помещения от утечки по инфракрасному каналу с помощью поискового прибора ST 031P «Пиранья»;

Лабораторная работа №3. Исследование уровней акустических сигналов защищаемого помещения

Лабораторная работа №4-5. Исследование методики акустической и виброакустической защиты помещения с помощью поискового прибора ST 031P «Пиранья»

Темы лабораторных работ 6 семестр:

Лабораторная работа №1. Исследование методики поиска закладных устройств нелинейным локатором «Родник-2К»;

Лабораторная работа №2. Исследование радиоэлектронной обстановки и радиоэлектронного канала утечки информации с помощью радиосканера «Icom IC-R1500».

Лабораторная работа №3. Расчет показателей защищенности конфиденциальной информации (расчет зоны R2) выделенного помещения с помощью программного комплекса «Гроза-К».

Лабораторная работа №4. Расчет показателей защищенности конфиденциальной информации (нормативных значений октавных соотношений «Сигнал/шум» при оценке защищенности выделенного помещения от утечки речевой конфиденциальной информации по электроакустическим каналам) с помощью программного комплекса «Гроза-К».

Темы лабораторных работ 7 семестр:

Лабораторная работа №1-2. Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;

Лабораторная работа №3-4. Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;

Лабораторная работа №5-6. 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 №7 Исследование методики защиты телефонных линий в помещении с помощью прибора проверки проводных линий «ULAN»;

Лабораторная работа №8. Исследование методики защиты телефонных линий в помещении с помощью прибора защиты телефонных переговоров «Прокруст 2000»;

Задание курсовой работы 7 семестр

Тема работы: «Моделирование технических каналов утечки информации на объекте, создание основной организационно-распорядительной документации службы безопасности» 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;
- Создание положения (устава) СБ объекта;
- Создание положений для всех структурных подразделениях СБ объекта;
- Создание инструкции по контрольно-пропускному и объектовому режиму предприятия (организации);
- Создание положения (инструкция) по обеспечению конфиденциальности информации в организации;
- Создание инструкции по ведению конфиденциального делопроизводства;
- Создание инструкции по обеспечению конфиденциальности информации при ее обработке на средствах вычислительной техники;
- Создание положения о коммерческой тайне предприятия (по вариантам);
- Создание инструкции по постоянно-действующей экспертной комиссии предприятия (по вариантам);

Вопросы и задания для самостоятельной работы студентов в 5 семестре:

- Демаскирующие признаки объектов защиты информации
- Источники и носители конфиденциальной информации
- Органы добывания информации
- Принципы добывания и обработки информации
- Оптические каналы утечки информации
- Радиоэлектронные каналы утечки
- Акустические каналы утечки
- Утечка информации через ПЭМИН
- Способы доступа к конфиденциальной информации
- Моделирование каналов защиты и объектов утечки информации

Вопросы и задания для самостоятельной работы студентов в 6 семестре:

- Технические средства акустической разведки
- Средства радиотехнической разведки
- Средства видовой разведки
- Методы поиска технических каналов утечки информации
- Методы акустической и виброакустической защиты
- Заземление и фильтрация сигналов
- Защита телефонных линий
- Противодействие электронным устройствам перехвата информации.
- Средства фильтрации сигналов. Методы и средства экранирования.
- Нелинейные локаторы. Методика поиска закладных устройств.

Вопросы и задания для самостоятельной работы студентов в 7 семестре:

- 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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Тельный, А.В. Технические средства охраны : практикум для вузов / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир :2012 .— 139 с.
2. Тельный, А.В.. Инженерно-техническая защита информации. Системы охранного телевидения : учебное пособие / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир 2013 .— 143 с.
3. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6
Режим доступа: <http://znanium.com/catalog.php?bookinfo=474838>

б) Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, Режим доступа: <http://znanium.com/catalog.php?bookinfo=405000>
2. Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.
3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. - 322 с. ISBN 978-5-369-01450-9. Режим доступа: <http://znanium.com/catalog.php?bookinfo=405000>
4. Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :

в) Периодические издания:

1. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: <http://inside-zi.ru/pages/about.html>;
2. Журнал «Спецтехника и Связь» , Режим доступа: <http://www.st-s.su/>

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.— Режим доступа: <http://edu.izi.vlsu.ru>
2. Информационная образовательная сеть.- Режим доступа: <http://ien.izi.vlsu.ru>
3. Внутривузовские издания ВлГУ.— Режим доступа: <http://e.lib.vlsu.ru/>
4. ИНТУИТ. Национальный открытый университет.— Режим доступа: <http://www.intuit.ru/>

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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 «Пирания-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.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01
"Информационная безопасность ", направленность «Комплексная защита объектов
информатизации»

Рабочую программу составил доц. кафедры ИЗИ к.т.н., Тельного А.В.

(ФИО, подпись)

Рецензент

(представитель работодателя) к.т.н. Вертилевский Н.В. РАЦ ООО «ИнфоЦентр»

Заместитель руководителя.

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 30.08.18 года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии
по направлению 10.03.01 "Информационная безопасность ", направленность «Комплексная
защита объектов информатизации»

Протокол № 1 от 30.08.18 года

Председатель комиссии д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

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

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № _____ от _____ 20__ г.

Заведующий кафедрой

(подпись, ФИО)

Актуализация рабочей программы дисциплины

(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

г) интернет-ресурсы: _____