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

УТВЕРЖДАЮ
Директор института
_____ А.А. Галкин
«__1__» ___09_____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОКОММУНИКАЦИЙ

Направление подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи»

Профиль/программа подготовки «Мобильные средства связи»

Уровень высшего образования: бакалавриат

Форма обучения очная

Владимир 2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: получение представления о современном несанкционированном доступе к информации и защите от него; выработка у студентов основных навыков в информационной защите предприятий и физических лиц от несанкционированного доступа;ознакомление студентов с основными видами несанкционированного доступа к конфиденциальной информации; знакомство с аппаратурными и программными методами борьбы с несанкционированным доступом.
Задачи: подготовка в области получения первичных знаний, умений и навыков студентов по основным принципам и методологии применения в области информационной безопасности для профессиональной деятельности специалиста: научно-исследовательской.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теория информационной безопасности и методология защиты инфокоммуникаций» относится к части, формируемой участниками образовательных отношений.

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	
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений	Знает :методы системного подхода для решения поставленных задач . Умеет осуществлять поиск, критический анализ и синтез информации. Владеет навыками и методами для применения системный подход для решения поставленных задач.	Тестовые вопросы
ПК-1 Способен осуществлять подготовку типовых технических проектов и первичный контроль соответствия разрабатываемых проектов и технической документации на различные инфокоммуникационные объекты национальным и	ПК-1.1. Знает принципы системного подхода в проектировании систем связи (телекоммуникаций) ПК-1.2. Знает современные технические решения создания объектов и систем связи (телекоммуникационных систем) и ее компонентов, новейшее оборудование и программное обеспечение ПК-1.3. Умеет использовать нормативно- техническую документацию при разработке проектной документации ПК-1.4. Владеет навыками	Знает назначение и возможности операционных систем Умеет создавать, редактировать и распечатывать текстовую информацию с помощью редактора Word, защищать документы Владеет поиском источников научно-технической информации (журналы, сайты Интернет), основными требованиями информационной безопасности	Тестовые вопросы

международным стандартам и техническим регламентам	оформления проектной документации в соответствии со стандартами и техническими регламентами		
ПК-2. Способен проводить предпроектную подготовку системного проекта телекоммуникационной системы	ПК-2.1. Знает современные требования по производительности, доступности, безопасности, масштабируемости, интеграции технологий, управляемости систем связи (телекоммуникаций) ПК-2.2. Умеет определять задачи, решаемые с помощью инфокоммуникационной системы и ожидаемые результаты ее использозования ПК-2.3. Владеет навыками сравнительного анализа и определения рисков, связанных с реализацией различных вариантов	Знает современные технические каналы утечки информации Умеет определять информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией Владеет навыками сравнительного анализа и определения рисков, связанных с реализацией защиты информации.	Тестовые вопросы
ПК-3. Способен проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ	ПК-3.1. Знает нормативно-правовые нормативно технические и организационно-методические документы, регламентирующие проектную подготовку, внедрение и эксплуатацию систем связи (теле коммуникационных систем), строительство объектов связи ПК-3.2. Знает принципы построения технического задания при автоматизации проектирования средств и сетей связи и их элементов; структуру и основы подготовки технической и проектной документации ПК-3.3. Умеет выявлять и анализировать преимущества и недостатки вариантов проектных решений, оценивать риски, связанные с реализацией проекта ПК-3.4. Умеет использовать современные информационно-коммуникационные технологии, в том числе специализированное программное обеспечение	Знает нормативно-правовые нормативно технические и организационно-методические документы, регламентирующие проектную подготовку, внедрение и эксплуатацию систем защиты информации Знает принципы построения технического задания при автоматизации проектирования средств и сетей связи и их элементов; структуру и основы подготовки технической и проектной документации при защите информации Умеет выявлять и анализировать преимущества и недостатки вариантов защиты информации, оценивать риски, связанные с реализацией проекта по защите информации. Умеет использовать современные информационно-коммуникационные технологии, в том числе специализированное	Тестовые вопросы

	для решения задач проектирования и проведения расчетов	программное обеспечение для решения задач проектирования и проведения расчетов при защите информации	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа

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.	Технические каналы утечки информации	6	1,-3	6			1	4	
2.	Демаскирующие признаки объектов	6	4,-6	6			1	5	Рейтинг-контроль (5нед)
3.	Средства выявления каналов утечки информации	6	7,-10	8		6	1	18	
4.	Скрытие и защита информации от утечки по техническим каналам	6	11-15	10		6	1	18	Рейтинг-контроль (11нед)
5.	Методы и средства инженерной защиты и технической охраны объектов	6	16-18	6		6	1	18	Рейтинг-контроль (17нед)
Всего за 6 семестр:				36		18		63	экзамен
Наличие в дисциплине КП/КР					-				
Итого по дисциплине									экзамен

Содержание лекционных занятий по дисциплине

Раздел 1. Технические каналы утечки информации

Тема 1Технические каналы утечки информации.

Структура, классификация и основные характеристики

Технические каналы утечки информации, обрабатываемой ТСПИ

Физическая природа побочных электромагнитных излучений.

Раздел 2. Демаскирующие признаки объектов

Тема 1 Общие положения

Демаскирующие признаки объектов

Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра

Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра

Демаскирующие признаки радиоэлектронных средств.

Раздел 3. Средства выявления каналов утечки информации

Тема 1 Общие сведения

Индикаторы электромагнитного поля

Сканирующие радиоприемники

Анализаторы спектра, радиочастотомеры

Многофункциональные комплекты для выявления каналов утечки информации.

Раздел 4 Скрытие и защита информации от утечки по техническим каналам

Тема 1 Концепция и методы инженерно-технической защиты информации

Экранирование электромагнитных волн.

Безопасность оптоволоконных кабельных систем

Заземление технических средств и подавление информационных сигналов в цепях заземления

Фильтрация информационных сигналов

Раздел 5. Методы и средства инженерной защиты и технической охраны объектов.

Тема 1Категории объектов защиты

Особенности задач охраны различных типов объектов

Общие принципы обеспечения безопасности объектов

Система охранно-тревожной сигнализации

Система контроля и управления доступом

Телевизионные системы

Система пожарной сигнализации

Периметровая охрана

Содержание лабораторных занятий по дисциплине

Лабораторная работа №1

Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении

Лабораторная работа №2

Обнаружение сигналов линейных и сетевых закладок

Лабораторная работа №3

Обнаружение оптических сигналов передатчиков ик-диапазона

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

Вопросы рейтинг – контроля №1

1В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

a) меры обеспечения целостности;

b) административные меры;

c) меры обеспечения конфиденциальности.

2. Дублирование сообщений является угрозой:

a) доступности;

b) конфиденциальности;

c) целостности.

3. Вредоносное ПО Melissa подвергает атаке на доступность:

a) системы электронной коммерции;

b) геоинформационные системы;

c) системы электронной почты.

4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

a) Melissa.

b) Bubble Boy.

c) ILO VE YOU.

5. Самыми опасными источниками внутренних угроз являются:

a) некомпетентные руководители;

b) обиженные сотрудники;

c) любопытные администраторы.

6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

a) просчеты при администрировании информационных систем;
b) необходимость постоянной модификации информационных систем;
c) сложность современных информационных систем.
7. Агрессивное потребление ресурсов является угрозой:
a) доступности
b) конфиденциальности
c) целостности
8. Программа Melissa — это:
a) бомба;
b) вирус;
c) червь.
9. Для внедрения бомб чаще всего используются ошибки типа:
a) отсутствие проверок кодов возврата;
b) переполнение буфера;
c) нарушение целостности транзакций.
10. Окно опасности появляется, когда:
a) становится известно о средствах использования уязвимости;
b) появляется возможность использовать уязвимость;
c) устанавливается новое ПО.

Вопросы рейтинг – контроля №2
11 .Среди ниже перечисленных отметьте две троянские программы:
a) I LOVE YOU;
b) Back Orifice;
c) Netbus.
12. Уголовный кодекс РФ не предусматривает наказания за:
a) создание, использование и распространение вредоносных программ;
b) ведение личной корреспонденции на производственной технической базе;
c) нарушение правил эксплуатации информационных систем.
13. Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:
a) средства выявления злоумышленной активности;
b) средства обеспечения отказоустойчивости;
c) средства контроля эффективности защиты информации.
14. Уровень безопасности В согласно «Оранжевой книге» характеризуется:
a) произвольным управлением доступом;
b) принудительным управлением доступом;
c) верифицируемой безопасностью.
15. В число классов требований доверия безопасности «Общих критериев» входят:
a) разработка;
b) оценка профиля защиты;
c) сертификация.
16. Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы:
a) периметр безопасности;
b) метки безопасности;
c) сертификаты безопасности.
17. Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:
a) управление квотами;
b) управление доступом;
c) экранирование.
18. Уровень безопасности А согласно «Оранжевой книге» характеризуется:
a) произвольным управлением доступом;
b) принудительным управлением доступом;
c) верифицируемой безопасностью.

19. Согласно рекомендациям X.800 аутентификация может быть реализована на:
a) сетевом уровне;
b) транспортном уровне;
c) прикладном уровне.
20. В число целей политики безопасности верхнего уровня входят:
a) решение сформировать или пересмотреть комплексную программу безопасности;
b) обеспечение базы для соблюдения законов и правил;
c) обеспечение конфиденциальности почтовых сообщений.
Вопросы рейтинг – контроля №3
21. В число целей политики безопасности верхнего уровня входят:
a) управление рисками;
b) определение ответственных за информационные сервисы;
c) определение мер наказания за нарушения политики безопасности.
22. В рамках политики безопасности нижнего уровня осуществляются:
a) стратегическое планирование;
b) повседневное администрирование;
c) отслеживание слабых мест защиты.
23. Политика безопасности строится на основе:
a) общих представлений об ИС организации;
b) изучения политик родственных организаций;
c) анализа рисков.
24. В число целей политики безопасности верхнего уровня входят:
a) формулировка административных решений по важнейшим аспектам реализации программы безопасности;
b) выбор методов аутентификации пользователей;
c) обеспечение базы для соблюдения законов и правил.
25. Риск является функцией:
a) размера возможного ущерба;
b) числа пользователей информационной системы;
c) уставного капитала организации.
26. В число этапов управления рисками входят:
a) идентификация активов;
b) ликвидация пассивов;
c) выборобъектов оценки.
27. Первый шаг в анализе угроз — это:
a) идентификация угроз;
b) аутентификация угроз;
c) ликвидация угроз.
28. Управление рисками включает в себя следующие виды деятель ности:
a) определение ответственных за анализ рисков;
b) оценка рисков;
c) выбор эффективных защитных средств.
29. Оценка рисков позволяет ответить на следующие вопросы:
a) чем рискует организация, используя информационную систе му?
b) чем рискуют пользователи информационной системы?
c) чем рискуют системные администраторы?
30. В число классов мер процедурного уровня входят:
a) поддержание работоспособности;
b) поддержание физической формы;
c) физическая защита.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Вопросы к экзамену

1. Технические каналы утечки информации.
2. Структура, классификация и основные характеристики
3. Технические каналы утечки информации, обрабатываемой ТСПИ
4. Физическая природа побочных электромагнитных излучений.
5. Демаскирующие признаки объектов
6. Демаскирующие признаки объектов
7. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра
8. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра
9. Демаскирующие признаки радиоэлектронных средств.
10. Средства выявления каналов утечки информации
11. Индикаторы электромагнитного поля
12. Сканирующие радиоприемники
13. Анализаторы спектра, радиочастотомеры
14. Многофункциональные комплекты для выявления каналов утечки информации.
15. Скрытие и защита информации от утечки по техническим каналам
16. Концепция и методы инженерно-технической защиты информации
17. Экранирование электромагнитных волн.
18. Безопасность оптоволоконных кабельных систем
19. Заземление технических средств и подавление информационных сигналов в цепях заземления
20. Фильтрация информационных сигналов
21. Методы и средства инженерной защиты и технической охраны объектов.
22. Категории объектов защиты
23. Особенности задач охраны различных типов объектов
24. Общие принципы обеспечения безопасности объектов
25. Система охранно-тревожной сигнализации
26. Система контроля и управления доступом
27. Телевизионные системы
28. Система пожарной сигнализации
29. Периметровая охрана
30.
    1. .

5.3. Самостоятельная работа обучающегося

Темы для докладов:

Проблемы развития теории и практики обеспечения информационной Безопасности

Основные понятия и определения в области информационной Безопасности

Определение информационной безопасности в свете информационных проблем современного общества

Основные составляющие информационной безопасности

Значение информационной безопасности для субъектов информационных отношений

Составляющие национальных интересов российской федерации в информационной сфере

Стратегия национальной безопасности российской федерации

Доктрина информационной безопасности российской федерации

Международное сотрудничество в области информационной безопасности: проблемы и перспективы

Концептуальная модель информационной безопасности

Информация как объект права собственности

Случайные угрозы

Преднамеренные угрозы

Модель гипотетического нарушителя информационной безопасности

Минимизация ущерба от аварий и стихийных бедствий

Дублирование информации

Повышение надежности информационной системы

Создание отказоустойчивых информационных систем

Оптимизация взаимодействия пользователей и обслуживающего персонала

Методы и средства защиты информации от традиционного шпионажа и
Методы и средства защиты от электромагнитных излучений и наводок
Защита информации от несанкционированного доступа

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. Азамов О.В. Информационная безопасность [Текст] / О. В. Азамов,К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин		http://www.naukaxxi.ru/materials/41/
2. Введение в информационную безопасность [Текст] / А.А. Малюк,В.С. Горбатов, В.И. Королев и др.; под ред. В.С. Горбатова. – М.:Горячая линия – Телеком, 2013. – 288 с.		https://e.lanbook.com/book/111075
n Гатчин Ю.А., Сухостат В.В. Теория информационной безопасностии методология защиты информации [Текст] / Ю.А. Гатчин, В.В.Сухостат – СПб., СПбГУ ИТМО, 2010. – 98 с.		https://books.ifmo.ru/book/587/teoriya_informacionnoy_bezopasnosti_i_metodologiya_zaschity_informacii.htm
Дополнительная литература		
1. ГОСТ Р 50922-2006: Защита информации. Основные термины иопределения		https://fintender.ru/star/gost/r-50922-2006
2. Доктрина информационной безопасности Российской Федерации[Текст]./ Указ Президента Российской Федерации от 5 декабря 2016г. №646		https://rg.ru/2016/12/06/doktrinainfobezobasnost-site-dok.html

6.2. Периодические издания

Отечественные журналы:
- Радиотехника;
- Радиотехника и электроника;
- Приборы и техника эксперимента;
- Цифровая обработка сигналов.

Реферативные журналы:
- Радиотехника;
- Электроника.

Зарубежные журналы:
- IEEE Transactions on Communications;
- IEEE Transactions on Signal Processing;
- IEEE Transactions on Instrumentation and Measurement.

6.3. Интернет-ресурсы

1. Журнал "Проектирование и технология электронных средств" - http://ptes.vlsu.ru
2. Журнал "Радиотехника" - http://radiotec.ru/catalog.php?cat=jr11
3. http://www.studentlibrary.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий практического типа. Лабораторные работы проводятся в компьютерных классах в ауд. 410-3 и 228-3.

Рабочую программу составил: к.т.н. доцент каф. РТ и РС _____ Н.Н.Корнеева

Рецензент:

Генеральный директор ОАО ВКБР к.т.н. _____ Богданов А.Е.

Программа рассмотрена и одобрена на заседании кафедры радиотехники и радиосистем

Протокол № 1 от 30.08.21 года

Заведующий кафедрой _____ Никитин О.Р.

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 11.03.02 - Инфокоммуникационные технологии и системы связи

Протокол № 1 от 1.09.21 года

Председатель комиссии _____ Никитин О.Р.

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

НАИМЕНОВАНИЕ

образовательной программы направления подготовки *код и наименование ОП*, направленность:

наименование (указать уровень подготовки)

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

Зав. кафедрой_____ / _____

Подпись *ФИО*