

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»**

Радиофизический факультет
(факультет / институт / филиал)

УТВЕРЖДЕНО
президиумом Ученого совета ННГУ
протокол от
«14» декабря 2021 г. № 4

Рабочая программа дисциплины

Проектирование защищенных
телекоммуникационных систем
(наименование дисциплины (модуля))

Уровень высшего образования
специалитет
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
10.05.02 Информационная безопасность телекоммуникационных систем
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Системы подвижной цифровой защищенной связи
(указывается профиль / магистерская программа / специализация)

Форма обучения

очная
(очная / очно-заочная / заочная)

Нижегород

2022 год

1. Место дисциплины в структуре ООП

Дисциплина «Проектирование защищенных телекоммуникационных систем» относится к дисциплинам обязательной части основной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
1	Блок 1. Дисциплины (модули) Обязательная часть	Дисциплина Б1.О.35 «Проектирование защищенных телекоммуникационных систем» относится к обязательной части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
ОПК-8 Способен применять методы научных исследований при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных систем и сетей	ОПК-8.1. Знает: - основные понятия теории познания - основные формы, методы и приемы научного исследования - структуру и методы научного эксперимента	Знать: - формы, методы и приемы научного исследования - структуру и методы научного эксперимента	Собеседование
	ОПК-8.2. Умеет: - составлять и оформлять простейшие виды научных трудов и их элементы	Уметь: - составлять научные труды и отчеты	Задачи (практические задания)
ОПК-16 Способен проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания	ОПК-16.1. Знает: - общие принципы проектирования современных систем и сетей телекоммуникаций - общие принципы построения защищенных систем и сетей телекоммуникаций - номенклатуру и содержание основных нормативных и методических	Знать: - принципы проектирования информационных систем и сетей телекоммуникаций - принципы построения защищенных информационных систем - нормативные документы по методам и средствам обеспечения информационной безопасности телекоммуникационных систем - методы оценки защищенности сетевого оборудования - формы технико-экономического обоснования проекта телекоммуникационной системы	Собеседование

<p>телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений</p>	<p>документов по методам и средствам обеспечения информационной безопасности телекоммуникационных систем</p> <ul style="list-style-type: none"> - существующие подходы к оценке защищенности сетевого оборудования и телекоммуникационных систем - место технико-экономического обоснования в жизненном цикле проектируемых систем - содержание технико-экономического обоснования проектируемой телекоммуникационной системы, ее элементов 		
	<p>ОПК-16.2. Умеет:</p> <ul style="list-style-type: none"> - проводить анализ показателей качества проектируемых сетей и систем телекоммуникаций - формировать требования к проектируемой системе с учетом анализа угроз защищаемым активам телекоммуникационной системы - формировать исходные данные для выполнения технико-экономического обоснования проектируемой телекоммуникационной системы 	<p>Уметь:</p> <ul style="list-style-type: none"> - анализировать показатели качества проектируемых сетей и систем - определять требования к проектируемой системе с учетом анализа угроз - формировать исходные данные для выполнения технико-экономического обоснования проектируемой телекоммуникационной системы 	<p>Задачи (практические задания)</p>
	<p>ОПК-16.3. Владеет:</p> <ul style="list-style-type: none"> - навыками создания компонентов защищенных телекоммуникационных систем 	<p>Владеть:</p> <ul style="list-style-type: none"> - навыками создания защищенных телекоммуникационных систем 	<p>Задачи (практические задания)</p>

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	5 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	180		
в том числе			
аудиторные занятия (контактная работа):			
- занятия лекционного типа	32		
- занятия семинарского типа (практические занятия / лабораторные работы)	16		
самостоятельная работа	76		
КСР	2		
Промежуточная аттестация – экзамен/зачет	экзамен 54		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего (часы)	В том числе				
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Нормативная база в области проектирования защищенных телекоммуникационных систем и обеспечения информационной безопасности	12	4			4	8
2. Основные понятия в области проектирования	14	4			4	10

защищенных телекоммуникационных систем и обеспечения информационной безопасности						
3. Характеристики наиболее распространенных угроз безопасности ЗТКС	18	4			4	14
4. Этапы разработки системы защиты информации, обеспечение надежного функционирования СЗИ. Построение модели угроз ЗТКС	42	10		16	26	16
5. Управление системой защиты информации в телекоммуникационной системе	20	6			6	14
6. Критерии надежности и эффективности функционирования СЗИ ЗТКС	18	4			4	14
Итого:	124	32		16	48	76

Текущий контроль успеваемости реализуется в рамках занятий, лабораторного типа.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя изучение дополнительных разделов дисциплины с использованием учебной литературы.

Для студентов разработаны презентационные материалы, а также учебно-методическое пособие «Планирование защитных мер телекоммуникационных систем», в которое вынесены вопросы изучения методов обеспечения безопасности ЗТКС. Материалы пособия дополняются разделами из списка рекомендованной литературы.

Текущий контроль усвоения материала проводится путем проведения опроса.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько незначительных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными незначительными недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка	Уровень подготовки
превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1. Контрольные вопросы

<i>Вопросы</i>	<i>Код формируемой компетенции</i>
1. Основные нормативно-правовые акты по защите конфиденциальной информации.	ОПК-8, ОПК-16
2. Понятия защищаемая информация, защита информации от утечки.	ОПК-8
3. Понятия: защита информации от несанкционированного доступа (НСД), защита информации от технической разведки, техническая защита конфиденциальной информации (ТЗКИ).	ОПК-8
4. Внешние и внутренние источники угроз безопасности информации.	ОПК-8
5. Понятие классификации объектов информатизации.	ОПК-8
6. Типовые объекты информатизации.	ОПК-8
7. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.	ОПК-8
8. Принципы разграничения доступа.	ОПК-8
9. Дайте определение технического канала утечки информации.	ОПК-8
10. В чем отличие основных технических средств (ОТСС) от вспомогательных технических средств и систем (ВТСС)?	ОПК-8, ОПК-16

11. Дайте определение контролируемой зоны (КЗ).	ОПК-8
12. Определения аттестации объектов информатизации по требованиям безопасности информации и сертификации, что общего, в чем различие.	ОПК-8, ОПК-16
13. Понятие объекта информатизации и автоматизированной системы.	ОПК-8, ОПК-16
14. Понятия: информация, документ, безопасность информации.	ОПК-8
15. Понятия: техническая защита конфиденциальной информации, защита информации от НСД.	ОПК-8
16. Понятия классификации и типизации, основные составляющие.	ОПК-8
17. Понятия инвентаризации и категорирования, основные задачи инвентаризации.	ОПК-8
18. Источники угроз безопасности информации.	ОПК-8
19. Дать понятие актуальной угрозы безопасности информации.	ОПК-8
20. Уязвимости, используемые в атаках.	ОПК-8
21. Понятия цели и задачи защиты информации.	ОПК-8, ОПК-16
22. Понятие программного (программно-математического) воздействия, группы угроз ПМВ.	ОПК-8, ОПК-16
23. Порядок организации ТЗИ на этапе определения замысла защиты.	ОПК-16
24. Принципы разграничения доступа.	ОПК-16
25. Общая классификация способов, мер и средств защиты от НСД.	ОПК-16
26. Содержание замысла защиты информации.	ОПК-16
27. Содержание концепции защиты информации.	ОПК-16
28. Меры и средства защиты от физического доступа.	ОПК-16
29. Меры и средства защиты от ПМВ.	ОПК-16
30. Порядок выбора целесообразных мер и средств защиты.	ОПК-16
31. Понятие системы защиты информации на объекте информатизации.	ОПК-16
32. На основании каких документов разрабатывается Модель угроз безопасности информации?	ОПК-16
33. Порядок разработки модели угроз безопасности, основные этапы.	ОПК-16
34. Как определяется исходный уровень защищенности ИСПДн.	ОПК-16
35. Нормативные документы ФСБ России по защите персональных данных и разработке модели нарушителя.	ОПК-16
36. Нормативные документы по разработке ТЗ на создание АС в защищенном исполнении.	ОПК-16
37. Понятия надежности, отказа, критериев отказа.	ОПК-16
38. Виды показателей долговечности и ремонтпригодности.	ОПК-16
39. Классификация объектов по показателям и методам оценки надежности.	ОПК-16

5.2.2. Типовые задания для оценки сформированности компетенции ОПК-8

1. Понятие угрозы безопасности информации.
2. Классификация угроз безопасности информации.
3. Порядок организации ТЗИ на этапе оценки обстановки.
4. Стратегии защиты информации в компьютерной сети.
5. Дерево отказов, его назначение.

6. Признаки классификации.
7. Принципы организации ТЗИ.
8. Классы защиты информации в СВТ.
9. Классы защиты информации в АС.

5.2.3. Типовые задания для оценки сформированности компетенции ОПК-16

1. Состав возможных уязвимых звеньев.
2. Общий алгоритм организации ТЗИ на объекте информатизации.
3. Объекты защиты на объекте информатизации.
4. Технологии (способы) создания доверенной среды.
5. Меры и средства защиты информации от утечки по ПЭМИН.
6. Меры и средства защиты от НСД с применением программных и программно-аппаратных средств.
7. Меры и средства защиты информации от техногенных угроз.
8. Документы по организации ТЗИ на объекте информатизации.
9. Порядок разработки модели нарушителя, основные этапы.
10. Виды показателей надежности и безотказности.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учебное пособие для вузов. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.

б) дополнительная литература:

1. Малюк А.А., Пазинин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.
2. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ В.А. Мокляков

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «09» декабря 2021 года, протокол № 07/21.