

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)

УТВЕРЖДАЮ:

Декан \_\_\_\_\_ Матросов В.В.

« 29 » \_\_\_\_\_ июня 2020 г.

**Рабочая программа дисциплины**

Б1.Б.38 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)

Квалификация (степень)

специалист

(бакалавр / магистр / специалист)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2018

## **1. Место и цели дисциплины в структуре ОПОП**

Дисциплина «Проектирование защищенных телекоммуникационных систем» относится к дисциплинам базовой части основной профессиональной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», преподается в 10 семестре.

Изучение студентами дисциплины «Проектирование защищенных телекоммуникационных систем» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Сети и системы передачи информации», «Операционные системы», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

### **Цели освоения дисциплины.**

Дисциплина «Проектирование защищенных телекоммуникационных систем» имеет целью раскрыть научные, методологические и законодательные основы организации системы защиты информации в телекоммуникационных системах, сформировать у студентов знания о базовых принципах и подходах к проектированию защищенных телекоммуникационных систем (ЗТКС), включая навыки по анализу и расчету показателей качества проектируемых ЗТКС, а также обеспечению функционирования и контролю эффективности.

### **Основными задачами дисциплины являются:**

- научить студентов основным принципам организации и этапам разработки системы защиты информации (СЗИ), определяющим стратегию обеспечения информационной безопасности и перечню правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности на телекоммуникационном предприятии;
- выработать навыки определения состава защищаемой информации и объектов защиты, выявления угроз, источников воздействия нарушителей, потерь;
- сформировать умения построения модели нарушителя, определяемой на основе обследования ресурсов системы и способов их использования;
- дать понятия модели угроз безопасности и оценку рисков, связанных с их осуществлением, получаемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;
- сформулировать требования безопасности, определяемые по результатам анализа рисков;
- научить выбирать компоненты СЗИ и определять условия их функционирования;
- выработать меры обеспечения информационной безопасности организационного и программно-технического уровня, предпринимаемые для реализации СЗИ;
- научить решать задачи проектирования СЗИ: технологического и организационного построения, кадрового обеспечения, материально-технического и нормативно-методического обеспечения;
- научить организовывать системы управления и контроля функционирования СЗИ, оценивать эффективность созданной СЗИ.

## 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК-1. Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем.	31 (ПК-1). Знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, основные нормативные и методические материалы; 32 (ПК-1). Знать источники и классификацию угроз информационной безопасности. У1 (ПК-1). Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. У2 (ПК-1). Уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, применять при проектировании защищенных телекоммуникационных систем соответствующие нормативные документы. В1 (ПК-1). Владеть навыками использования при проектировании защищенных телекоммуникационных систем нормативных документов.
ПК-3. Способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств.	31 (ПК-3). Знать основные угрозы ИБ телекоммуникационных систем, особенности их реализаций, классификацию видов атак и особенности их реализации. У1 (ПК-3). Уметь составлять функциональные схемы проектируемых систем и сетей телекоммуникаций. В1 (ПК-3). Владеть навыками составления проекта и пониманием содержания основных этапов процесса проектирования.
ПК-5. Способность проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов.	31 (ПК-5). Знать принципы проектирования защищенных телекоммуникационных систем и их элементы, проведения анализа проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания. У1 (ПК-5). Уметь проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техни-

	<p>ческую документацию с учетом действующих нормативных и методических документов.</p> <p>В1 (ПК-5). Владеть способностью проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов.</p>
<p>ПК-6. Способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду.</p>	<p>31 (ПК-6). Знать принципы технологий обеспечения информационной безопасности телекоммуникационных систем, нормы их интеграции в государственную и международную информационную среду.</p> <p>У1 (ПК-6). Уметь применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду.</p> <p>В1 (ПК-6). Владеть способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду.</p>
<p>ПК-7. Способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.</p>	<p>31 (ПК-7). Знать принципы выбора средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.</p> <p>У1 (ПК-7). Уметь осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.</p> <p>В1 (ПК-7). Владеть способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.</p>

### 3. Структура и содержание дисциплины «Проектирование защищенных телекоммуникационных систем»

Объем дисциплины составляет 4 зачетные единицы, всего 144 часа, из которых 50 часов составляет контактная работа обучающегося с преподавателем (32 часа занятия лекционного

типа, 16 часов занятия лабораторного типа, в том числе 2 часа – мероприятия текущего контроля успеваемости, 2 часа – мероприятия промежуточной аттестации), 94 часа составляет самостоятельная работа обучающегося.

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	8	4			4	8
2. Основные понятия в области проектирования защищенных телекоммуникационных систем и обеспечения информационной безопасности	10	4			4	10
3. Характеристики наиболее распространенных угроз безопасности ЗТКС	10	4			4	14
4. Этапы разработки системы защиты информации, обеспечение надежного функционирования СЗИ. Построение модели угроз ЗТКС	52	10		16	26	32
5. Управление системой защиты информации в телекоммуникационной системе	16	6			6	16
6. Критерии	12	4			4	14

надежности и эффективности функционирования СЗИ ЗТКС						
В т.ч. текущий контроль	2			2	2	
Промежуточная аттестация: экзамен						

#### 4. Образовательные технологии

**Образовательные технологии, способствующие формированию компетенций.**

**используемые на занятиях лекционного типа:**

- лекции с изложением учебного материала.

**используемые на занятиях практического типа:**

- решение конкретных проблемных ситуаций в сфере информационной безопасности телекоммуникационных систем с использованием технологии коллективной мыслительной деятельности.

#### 5. Учебно-методическое обеспечение самостоятельной работы обучающихся

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. Контроль за процессом усвоения материала осуществляется с помощью контрольных вопросов.

#### 6. Фонд оценочных средств для промежуточной аттестации по дисциплине, включающий:

**6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.**

Индикаторы компетенции	Критерии оценивания						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
<u>Знания</u>	Отсутствие знаний материала	Наличие грубых ошибок в основном материале	Знание основного материала с рядом негрубых ошибок	Знание основного материала с рядом заметных погрешностей	Знание основного материала с незначительными и погрешностями	Знание основного материала без ошибок и погрешностей	Знание основного и дополнительного материала без ошибок и погрешностей

							ностей
<u>Умения</u>	Отсутствует способность решения стандартных задач	Наличие грубых ошибок при решении стандартных задач	Способность решения основных стандартных задач с существенными ошибками	Способность решения всех стандартных задач с незначительными погрешностями	Способность решения всех стандартных задач без ошибок и погрешностей	Способность решения стандартных и некоторых нестандартных задач	Способность решения стандартных задач и широкого круга нестандартных задач
<u>Навыки</u>	Полное отсутствие навыка	Отсутствие навыка	Владение навыком в минимальном объеме	Посредственное владение навыком	Достаточное владение навыком	Хорошее владение навыком	Всестороннее владение навыком

## 6.2. Описание шкал оценивания.

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена.

### Критерии оценок.

Оценка	Уровень подготовки
Превосходно	Высокий уровень подготовки, безупречное владение теоретическим материалом, студент демонстрирует творческий подход к решению нестандартных ситуаций. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами. Студент активно работал на лабораторных занятиях.
Отлично	Высокий уровень подготовки с незначительными ошибками. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами. Студент активно работал на лабораторных занятиях.
Очень хорошо	Хорошая подготовка. Студент дает ответ на все теоретические вопросы билета при наличии неточностей. Студент активно работал на лабораторных занятиях.
Хорошо	В целом хорошая подготовка с заметными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы билета при наличии неточностей. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора. Студент работал на лабораторных занятиях.
Удовлетворительно	Минимально достаточный уровень подготовки. Студент показывает минимальный уровень теоретических знаний, делает существенные ошибки, но при ответах на наводящие вопросы, может правильно сориентироваться и в общих чертах дать правильный ответ. Студент посещал лабораторные занятия.

Неудовлетворительно	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы экзаменатора.
Плохо	Подготовка абсолютно недостаточная. Студент не отвечает на поставленные вопросы.

### **6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.**

Для оценивания результатов обучения в виде **знаний** используются следующие процедуры и технологии: экзамен, проводимый в письменной форме с дальнейшим индивидуальным собеседованием.

Для оценивания результатов обучения в виде **умений** и **навыков** используются следующие процедуры и технологии: проверка отчета, составляемого по результатам выполнения заданий лабораторного практикума.

### **6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.**

#### **Типовые задания для текущего контроля успеваемости.**

##### **6.4.1. Задания для оценки компетенции «ПК-1», «ПК-7»:**

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.

##### **6.4.2. Задания для оценки компетенции «ПК-3», «ПК-5», «ПК-6»:**

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.

#### **Типовые задания (оценочные средства), выносимые на экзамен.**

##### **6.4.3. Задания для оценки компетенции «ПК-1»:**

1. Основные нормативно-правовые акты по защите конфиденциальной информации.



2. Понятия защищаемая информация, защита информации от утечки.
3. Понятия: защита информации от несанкционированного доступа (НСД), защита информации от технической разведки, техническая защита конфиденциальной информации (ТЗКИ).
4. Внешние и внутренние источники угроз безопасности информации.
5. Понятие классификации объектов информатизации.
6. Принципы разграничения доступа.
7. Дайте определение технического канала утечки информации.
8. В чем отличие основных технических средств (ОТСС) от вспомогательных технических средств и систем (ВТСС)?
9. Дайте определение контролируемой зоны (КЗ).
10. Понятие объекта информатизации и автоматизированной системы.
11. Понятия: информация, документ, безопасность информации.
12. Понятия: техническая защита конфиденциальной информации, защита информации от НСД.
13. Понятия: классификации и типизации, основные составляющие.
14. Понятия инвентаризации и категорирования, основные задачи инвентаризации.
15. Источники угроз безопасности информации.
16. Дать понятие актуальной угрозы безопасности информации.
17. Уязвимости, используемые в атаках.
18. Понятия цели и задачи защиты информации.
19. Понятие программного (программно-математического) воздействия, группы угроз ПМВ.
20. Принципы разграничения доступа.
21. Содержание замысла защиты информации.
22. Содержание концепции защиты информации.
23. Порядок разработки модели угроз безопасности, основные этапы.
24. Как определяется исходный уровень защищенности ИСПДн?
25. Понятия надежности, отказа, критериев отказа.
26. Виды показателей долговечности и ремонтпригодности.

#### 6.4.4. Задания для оценки компетенции «ПК-3»:

1. Типовые объекты информатизации.
2. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.
3. Определения аттестации объектов информатизации по требованиям безопасности информации и сертификации, что общего, в чем различие.
4. Порядок организации ТЗИ на этапе определения замысла защиты.
5. Общая классификация способов, мер и средств защиты от НСД.
6. Меры и средства защиты от физического доступа.
7. Меры и средства защиты от ПМВ.
8. Порядок выбора целесообразных мер и средств защиты.
9. Понятие системы защиты информации на объекте информатизации.
10. На основании каких документов разрабатывается Модель угроз безопасности информации?
11. Нормативные документы ФСБ России по защите персональных данных и разработке модели нарушителя.
12. Нормативные документы по разработке ТЗ на создание АС в защищенном исполнении.
13. Классификация объектов по показателям и методам оценки надежности.

#### 6.4.5. Задания для оценки компетенции «ПК-5»:

1. Типовые объекты информатизации.

2. Определения аттестации объектов информатизации по требованиям безопасности информации и сертификации, что общего, в чем различие.
3. Понятие объекта информатизации и автоматизированной системы.
4. Меры и средства защиты от физического доступа.
5. Меры и средства защиты от ПМВ.
6. Порядок выбора целесообразных мер и средств защиты.
7. Как определяется исходный уровень защищенности ИСПДн.

6.4.6. Задания для оценки компетенции «ПК-6»:

1. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.
2. Понятия: информация, документ, безопасность информации.
3. Понятия: техническая защита конфиденциальной информации, защита информации от НСД.
4. Понятия классификации и типизации, основные составляющие.
5. Понятия инвентаризации и категорирования, основные задачи инвентаризации.
6. Классификация объектов по показателям и методам оценки надежности.

6.4.7. Задания для оценки компетенции «ПК-7»:

1. В чем отличие основных технических средств (ОТСС) от вспомогательных технических средств и систем (ВТСС)?
2. Источники угроз безопасности информации.
3. Понятие программного (программно-математического) воздействия, группы угроз ПМВ.
4. Порядок организации ТЗИ на этапе определения замысла защиты.

**6.5. Методические материалы, определяющие процедуры оценивания.**

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утвержденное приказом ректора ННГУ от 13.02.2014 г. №55-ОД.

Положение «О фонде оценочных средств», утвержденное приказом ректора ННГУ от 10.06.2015 г. №247-ОД.

## **7. 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.

## **8. Материально-техническое обеспечение дисциплины**

Аудиторный фонд ННГУ для проведения лекций.

Компьютерные класс лаборатории «Средства коммуникаций и безопасность информационных систем».

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) \_\_\_\_\_ В.А. Мокляков

Рецензент (ы) \_\_\_\_\_ С.Н. Жуков

Заведующий кафедрой «Безопасность  
информационных систем» \_\_\_\_\_ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» июня 2020 года, протокол № 03/20.