

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

Комплексное обеспечение защиты информации
(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 «Комплексное обеспечение защиты информации» 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.36 «Комплексное обеспечение защиты информации» 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-6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Знает: - цели и задачи управленческой деятельности - принципы, методы, формы управленческой деятельности - функции управления и этапы реализации процесса управления - основные угрозы безопасности информации и модели нарушителя в телекоммуникационных системах - принципы формирования политики информационной безопасности телекоммуникационной системы - задачи органов защиты государственной тайны и служб защиты информации на предприятиях - систему	Знать: - цели и задачи управленческой деятельности - принципы, методы, формы управленческой деятельности - функции управления и этапы реализации процесса управления - основные угрозы безопасности информации и модели нарушителя в телекоммуникационных системах - принципы формирования политики информационной безопасности телекоммуникационной системы - задачи органов защиты государственной тайны и служб защиты информации на предприятиях - систему организационных мер, направленных на защиту информации ограниченного доступа	Собеседование

	организационных мер, направленных на защиту информации ограниченного доступа		
	ОПК-6.2. Умеет: - составлять и оформлять основные документы планирования и отчетные документы исполнителя и руководителя первичного звена - проводить анализ состава и функциональных возможностей средств защиты информации телекоммуникационной системы в целях его совершенствования - разрабатывать модели угроз и модели нарушителя информационной безопасности телекоммуникационной системы - формулировать основные требования, предъявляемые к организации защиты информации ограниченного доступа	Уметь: - составлять и оформлять основные документы планирования и отчетные документы исполнителя и руководителя первичного звена - проводить анализ состава и функциональных возможностей средств защиты информации телекоммуникационной системы в целях его совершенствования - разрабатывать модели угроз и модели нарушителя информационной безопасности телекоммуникационной системы - формулировать основные требования, предъявляемые к организации защиты информации ограниченного доступа	Собеседование. Задачи (практические задания)
ОПК-15 Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	ОПК-15.1. Знает: - методики измерения и оценки параметров в телекоммуникационных системах	Знать: - методики измерения и оценки параметров в телекоммуникационных системах	Собеседование
	ОПК-15.2. Умеет: - проводить измерения в спектральной и временной области - анализировать пропускную способность и предельную нагрузку сети связи - анализировать параметры передачи кадров при прохождении по каналам связи - проверять достижимость абонентов сети связи - выявлять трафик сетевых атак	Уметь: - проводить измерения в спектральной и временной области - анализировать пропускную способность и предельную нагрузку сети связи - анализировать параметры передачи кадров при прохождении по каналам связи - проверять достижимость абонентов сети связи - выявлять трафик сетевых атак	Собеседование. Задачи (практические задания)

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	6 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	216		
в том числе			
аудиторные занятия (контактная работа):			
- занятия лекционного типа	32		
- занятия семинарского типа (практические занятия / лабораторные работы)	32		
самостоятельная работа	105		
КСР	2		
Промежуточная аттестация – экзамен/зачет	экзамен 45		

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. Принципы организации КСЗИ. Задачи комплексной системы защиты информации	14	4			4	10
2. Системный подход в создании КСЗИ. Требования к КСЗИ	16	4			4	12
3. Обобщенная модель защищенной системы. Этапы разработки и жизненный цикл КСЗИ	20	4			4	16
4. Определение объектов защиты. Анализ и оценка угроз безопасности информации. Модель гипотетического нарушителя	24	6			6	18
5. Потенциальные каналы, методы и возможности НСД к информации	40	6		16	22	18
6. Классификация мер обеспечения безопасности компьютерных систем. Компоненты КСЗИ	21	4			4	17
7. Подсистемы ЗИ. Модели оценки эффективности КСЗИ. Контроль функционирования КСЗИ	34	4		16	20	14
Итого:	169	32		32	64	105

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 несущественных 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	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но	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 несущественным недочетами, выполнены все задания в	Продemonстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

			объеме.	некоторые с недочетами.		полном объеме.	
<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 ошибок и 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

Вопросы	Код формируемой компетенции
1. Технология разработки программного обеспечения.	ОПК-6
2. Алгоритмические и программные закладки.	ОПК-6

3. Объекты информационной системы, нуждающиеся в защите.	ОПК-6
4. Методика их выявления. Объектов, нуждающихся в защите.	ОПК-6
5. Анализ рисков.	ОПК-6
6. Что такое аудит информационной безопасности.	ОПК-6
7. Идентификация адреса абонента в сети и установление соединения.	ОПК-6
8. Аппаратные средства защиты информации.	ОПК-6, ОПК-15
9. Аппаратные средства защиты информации.	ОПК-6, ОПК-15
10. Организация защиты информации в исследовательских учреждениях.	ОПК-6, ОПК-15
11. Распределение обязанностей и организация работы в подразделении, обеспечивающем защиту информации.	ОПК-6, ОПК-15
12. Порядок и особенности внедрения КСИБ.	ОПК-15
13. Порядок и особенности проведения испытаний и внедрения КСИБ.	ОПК-15
14. Организация хранения документов.	ОПК-6, ОПК-15
15. Организационные проблемы защиты информации.	ОПК-6, ОПК-15
16. Компоненты комплексной системы защиты информации.	ОПК-15
17. Методика определения состава защищаемой информации. Перечень сведений, составляющих коммерческую тайну.	ОПК-6, ОПК-15
18. Механизмы обеспечения безопасности информации: идентификация, авторизация, аудит, разграничение доступа.	ОПК-6, ОПК-15
19. Принципы построения комплексной системы защиты информации.	ОПК-6, ОПК-15
20. Разработка политики безопасности и регламенты информационной безопасности предприятия.	ОПК-6, ОПК-15

5.2.2. Типовые задания для оценки сформированности компетенции ОПК-6, ОПК-15

- Определить какой из перечисленных ниже способов управления рисками является наименее желательным:
 - принятие риска;
 - уменьшение риска;
 - передача риска;
 - отказ от риска.
- Определить необходимые меры, если в компании не хватает финансовых средств на исключение всех уязвимостей:
 - предложить руководству изыскать дополнительные средства, объяснив уголовную ответственность руководства и обосновав окупаемость контрмер;
 - сосредоточиться на наиболее критичных уязвимостях;
 - уделить внимание всем уязвимостям в равной степени, чтобы каждая уязвимость могла иметь хоть какую-нибудь защиту;

d) используя принцип «скрытия данных по ИБ», постараться замолчать указанную проблему до лучших времен.

3. Определить документы по ИБ, имеющие обязательный характер в организации:

- a) профили защиты;
- b) рекомендательные письма от известных родителей;
- c) руководящие указания;
- d) стандарты организации.

4. Определить меры, имеющие первостепенное значение при организации системы защиты:

- a) выбор эффективных средств скрытого наблюдения;
- b) информирование и организация эффективного обучения;
- c) одобрение руководством;
- d) разработка ценных указаний.

6. Учебно-методическое и информационное обеспечение дисциплины

a) основная литература:

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.
2. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учебное пособие для вузов. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.
3. Барабанов Л.В., Дорофеев Л.В., Марков А.С, Цирлов В.Л. Семь безопасных информационных технологий/под ред. А.С. Маркова. - М.: ДМК Пресс, 2017.- 224 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.