

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.39 Информационная безопасность
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 «Информационная безопасность 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 «Информационная безопасность телекоммуникационных систем» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Сети и системы передачи информации», «Архитектура вычислительных систем», «Операционные системы», «Основы информационной безопасности».

Цели освоения дисциплины

Содержание дисциплины направлено на ознакомления студентов с основными уязвимостями телекоммуникационных систем на различных уровнях модели взаимодействия OSI, методами и средствами защиты информации, передаваемой по сети.

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. (этап освоения: завершающий)	31 (ПК-1). Источники и классификацию угроз информационной безопасности. 32 (ПК-1). Основные уязвимости программно-аппаратных компонентов информационно-телекоммуникационных систем. У1 (ПК-1). Классифицировать и оценивать угрозы для объекта информатизации. У2 (ПК-1). Анализировать и оценивать угрозы безопасности объекта У3 (ПК-1). Анализировать безопасность функционирования телекоммуникационных систем В1 (ПК-1). Навыками анализа сетевых протоколов. В2 (ПК-1). Навыками анализа безопасности функционирования телекоммуникационных систем.
ПК-3. Способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств	31 (ПК-3) возможности технических средств перехвата информации 32 (ПК-3). Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации 33 (ПК-3). Технологии, средства и методы

(этап освоения: завершающий)	<p>обеспечения информационной безопасности телекоммуникационных систем.</p> <p>У1 (ПК-3). Оценивать уязвимость протоколов и интерфейсов телекоммуникационных систем.</p> <p>У2 (ПК-3). Разрабатывать политики безопасности телекоммуникационных систем.</p> <p>В1 (ПК-3). Навыками безопасного использования технических средств в профессиональной деятельности.</p> <p>В2 (ПК-3). Навыками рационального выбора средств и методов защиты информации объектов информатизации</p>
------------------------------	---

3. Структура и содержание дисциплины «Информационная безопасность телекоммуникационных систем»

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из которых 49 часов составляет контактная работа обучающегося с преподавателем (16 часов занятия лекционного, 32 часа занятия лабораторного типа, в том числе 2 часа – мероприятия текущего контроля успеваемости, 1 час – мероприятия промежуточной аттестации), 59 часов 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				Самостоятельная работа обучающегося, часы
		из них				
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Классификация атак по уровням модели OSI	24	6		8	14	10
2. Атаки на сети Wi-Fi	20	2			2	18
3. Организация виртуальных частных сетей	31	3		16	19	12
4. Средства защиты сетевого уровня	20	2		8	10	10
5. Системы	12	3			3	9

обнаружения вторжений						
В т.ч.текущий контроль	2			2	2	
Промежуточная аттестация: Зачет						

4. Образовательные технологии

Образовательные технологии, способствующие формированию компетенций.

используемые на занятиях лекционного типа:

- лекции с изложением учебного материала.

используемые на занятиях практического типа:

- решение задач развертывания и настройки сетей с использованием технологии коллективной мыслительной деятельности.

5. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:

- изучение дополнительных разделов дисциплины с использованием учебной литературы;
 - изучение и проверка компьютерных настроек и интерфейсов на персональных компьютерах обучающихся.

Текущий контроль усвоения материала проводится путем проведения опроса.

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	
	«незачтено»	«зачтено»
<u>Знания</u>	Наличие грубых ошибок в основном материале	Знание основного материалом, возможно с рядом погрешностей
<u>Умения</u>	Наличие грубых ошибок при выполнении стандартных заданий	Способность выполнения всех стандартных заданий, возможно с незначительными погрешностями
<u>Навыки</u>	Отсутствие навыка	Достаточное владение навыком

6.2. Описание шкал оценивания.

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

Критерии оценок.

Оценка	Уровень подготовки
Зачтено	В целом хорошая подготовка с возможными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы. Студент работал на лабораторных занятиях.
Не зачтено	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные 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:

Зачет, 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. Задачи для оценки компетенции «ПК-3»:

Задача 1. Развернуть сегментированную сеть, используя технологию VLAN.

Задача 2. Построить виртуальную частную сеть, позволяющую осуществлять удаленный доступ.

Задача 3. Построить виртуальную частную сеть, позволяющую обеспечить туннель между удаленными сетями.

Типовые задания (оценочные средства), выносимые на зачет.

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

1. Атаки на физическом уровне модели ISO.
2. Атаки на коммутаторы Ethernet.
3. Атаки на протоколы VLAN.
4. Атаки на протокол STP.
5. Атаки на протокол ARP.
6. Атаки на протокол DHCP.
7. Атаки на протоколы маршрутизации.
8. Атаки на протоколы транспортного уровня.

9. Сканирование сети.
10. Атаки типа «Отказ в обслуживании».
11. Атаки на уровне приложений.
12. Протоколы защиты Wi-Fi.
13. Защита устройств беспроводных сетей.
14. Семейство протоколов IPSec.
15. Ассоциации безопасности и протоколы управления и обмена ключами.
16. Варианты построения виртуальных частных сетей.
17. Организация защиты от вирусов.
18. Межсетевые экраны сетевого уровня.
19. Межсетевые экраны уровня приложений.
20. Системы обнаружения вторжений.

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

1. Сканирование сети.
2. Защита устройств беспроводных сетей.
3. Варианты построения виртуальных частных сетей.
4. Организация защиты от вирусов.
5. Межсетевые экраны сетевого уровня.
6. Межсетевые экраны уровня приложений.
7. Системы обнаружения вторжений.

6.5. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утверждённое 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. Малышенко Ю. В., Федоров В. В. - Защита информации в вычислительных сетях, системах и комплексах: учеб. пособие по дисциплине "Информац. тамож. технологии". - М.: РИО РГА, 2007. - 108 с.

б) дополнительная литература:

1. Фороузан Б. А. - Криптография и безопасность сетей: учеб. пособие. - М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаб. знаний, 2010. - 784 с.

в) программное обеспечение и Интернет-ресурсы:

1. Программное обеспечение "Cisco Packet Tracer"

8. Материально-техническое обеспечение дисциплины

Аудиторный фонд ННГУ для проведения лекций.

Компьютерные класс лаборатории «Средств коммуникаций и безопасности 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) _____ А.А. Рябов

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.