МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ

Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УВР
_____ А.Г. Жуковский
«30» 12 2022 г.

Методы и средства защиты компьютерной информации
Б1.В.ДВ.09.01
рабочая программа дисциплины

Кафедра Инфокоммуникационные технологии и системы связи
Направление подготовки **09.03.01 Информатика и вычислительная техника**
Профиль **Интеллектуальные системы обработки информации**
Прикладные информационные системы и современные языки программирования
Формы обучения **очная, заочная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7	3	108/4
Контактная работа, в том числе (по семестрам, курсам):		48/7		14/4
Лекции		16/7		8/4
Лабораторных работ		16/7		
Практических занятий		16/7		6/4
Семинаров				
Самостоятельная работа		60/7		94/4
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам		1/7		1/4
Число экзаменов с разбивкой по семестрам				

Программу составил:
Доцент кафедры ИТСС, к.т н., доцент Манин А.А.

Рецензент(ы):
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Методы и средства защиты компьютерной информации»

Разработана в соответствии с ФГОС ВО
направления подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА,
утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 929.

Составлена на основании учебных планов
направления 09.03.01 Информатика и вычислительная техника, профилей «Интеллектуальные системы обработки информации», «Прикладные информационные системы и современные языки программирования», одобренных Учёным советом СКФ МТУСИ, протокол №5 от 26.12.2022, и утвержденных директором СКФ МТУСИ 26.12.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «8» 12 2022 г. № 4

Зав. кафедрой _____ Соколов С.В.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

1. Цели изучения дисциплины

Целями изучения дисциплины «Методы и средства защиты компьютерной информации» являются овладение совокупностью технологий, способов, средств и методов защиты компьютерной информации, циркулирующей в сетях связи.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

- ***технологическая деятельность****: приемка и освоение вводимого инновационного оборудования; монтаж, наладка, испытания и сдача в эксплуатацию опытных образцов изделий, узлов, и систем; внедрение и эксплуатация информационных систем; обеспечение защиты информации и объектов информатизации; разработка норм, правил и требований к технологическим процессам обмена информацией на расстоянии; организация мероприятий по охране труда и технике безопасности в процессе ввода в эксплуатацию, технического обслуживания и ремонта инфокоммуникационного оборудования; доведение инфокоммуникационных услуг до пользователей.*

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности
Знать:
Возможные угрозы НСД к компьютерным сетям; Сетевые протоколы и параметры настройки; Особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; Методы комплексного обеспечения защиты сетей; Нормативные правовые акты в области защиты информации; Национальные, межгосударственные и международные стандарты в области защиты информации.
Уметь:
Осуществлять организацию и проведение монтажа и настройки сетевого оборудования, а также средств и систем защиты от НСД; Использовать встроенные механизмы защиты от НСД в составе сетевого оборудования; Устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании.
Владеть:
Определение необходимого состава, особенностей размещения и функциональных возможностей сетевого оборудования, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; Организация и проведение монтажа и настройки сетевого оборудования, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; Контроль соответствия параметров подсистем защиты от НСД установленным требованиям, обеспечение своевременной корректировки настроек сетевого оборудования, средств и систем их защиты от НСД в целях реагирования на

выявленные нарушения.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.В.16 «Сети и телекоммуникации»
2	Б1.О.05 «Информатика»
3	Б1.О.12 «Архитектура информационных систем»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.03(Пд) «Производственная (проектно-технологическая) практика»
2	Б3.01. «Государственная итоговая аттестация»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 48 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 4 , Семестр 7					
Модуль 1 – Методы и средства защиты элементов сетей от НСД – 56 (28+28) часов					
1.1	Политика безопасности сети 1. Основные понятия 2. Дискреционная политика безопасности 3. Мандатная политика безопасности 4. Ролевая политика безопасности	Лек.	2	ПК-10	Л1.1
1.2	Защита от несанкционированного доступа к сетевому оборудованию 1. Защита консольного доступа 2. Протоколы удаленного доступа к оборудованию 3. Защита удаленного доступа	Лек.	2	ПК-10	Л1.1
1.3	Использование AAA-сервера для защиты удаленного доступа 1. Протокол RADIUS 2. Протокол TACACS+	Лек.	2	ПК-10	Л1.1
1.4	Межсетевое экранирование 1. Определение и классификация межсетевых экранов 2. Межсетевые экраны с пакетной фильтрацией 3. Межсетевые экраны с сохранением состояний 4. Межсетевые экраны Zone-Based Policy Firewall (ZBFW)	Лек.	2	ПК-10	Л1.1,
1.5	Конфигурирование консольного доступа к сетевому оборудованию	ПЗ1	4	ПК-10	Л3.1
1.6	Конфигурирование удаленного доступа к сетевому оборудованию	ПЗ2	4	ПК-10	Л3.1
1.7	Исследование свойств межсетевого экрана с пакетной фильтрацией	ЛР1	4	ПК-10	Л3.2
1.8	Исследование свойств межсетевого экрана с сохранением состояний	ЛР2	4	ПК-10	Л3.2
1.9	Исследование свойств межсетевого экрана ZBFW	ЛР3	4	ПК-10	Л3.2
1.10	Требования нормативных документов и технических регламентов к защищенным сетям связи	Ср.	8	ПК-10	Л2.2 Л2.3
1.11	Технические характеристики аппаратных межсетевых экранов различных производителей	Ср.	8	ПК-10	Л1.1
1.12	Обеспечение защиты беспроводного сетевого оборудования	Ср.	6	ПК-10	Л1.1
1.13	Механизмы комплексной защиты сетей электросвязи	Ср.	6	ПК-10	Л1.1

Модуль 2 – Защита корпоративных сетей от НСД – 52 (20+32)часа					
2.1	Защита периметра корпоративной сети 1. Защита периметра с применением межсетевого экранирования 2. Статический NAT. 3. Динамический NAT 4. NAT с применением маскарадинга	Лек.	4	ПК-10	Л1.1
2.2	Защита корпоративной информации, передаваемой по общедоступной сети 1. Определение и классификация VPN 2. Протоколы VPN, реализуемые на втором уровне модели OSI 3. Протоколы VPN, реализуемые на третьем уровне модели OSI 4. Протоколы туннелирования 5. Протоколы IPSec	Лек.	4	ПК-10	Л1.1
2.3	Конфигурирование NAT на маршрутизаторе	ПЗ3	8	ПК-10	Л3.1
2.4	Исследование VPN-туннеля	ЛР4	4	ПК-10	Л3.2
2.9	Механизмы защиты корпоративной сети от DoS-атак	Ср.	8	ПК-10	Л1.1
2.10	Механизмы защиты корпоративной сети от компьютерных вирусов	Ср.	8	ПК-10	Л1.1
2.11	Области применения технологий VPN второго уровня	Ср.	8	ПК-10	Л1.1
2.12	Организационные мероприятия по комплексной защите корпоративной сети	Ср.	8	ПК-10	Л1.1
Итого – 108 часов					

4.2 Заочная форма обучения, 5 лет (всего 108 часов, 14 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 4 , Семестр 8					
Модуль 1 – Методы и средства защиты элементов сетей от НСД – 52 (8+44) часов					
1.1	Политика безопасности сети 1. Основные понятия 2. Дискреционная политика безопасности 3. Мандатная политика безопасности 4. Ролевая политика безопасности	Лек.	2	ПК-10	Л1.1
1.2	Защита от несанкционированного доступа к сетевому оборудованию	Ср.	4	ПК-10	Л1.1
1.3	Использование AAA-сервера для защиты удаленного доступа	Ср.	4	ПК-10	Л1.1
1.4	Межсетевое экранирование 1. Определение и классификация межсетевых	Лек.	2	ПК-10	Л1.1,

	экранов 2. Межсетевые экраны с пакетной фильтрацией 3. Межсетевые экраны с сохранением состояний 4. Межсетевые экраны Zone-Based Policy Firewall (ZBFW)				
1.5	Конфигурирование консольного доступа к сетевому оборудованию	ПЗ1	1	ПК-10	Л3.1
1.6	Конфигурирование удаленного доступа к сетевому оборудованию	ПЗ2	1	ПК-10	Л3.1
1.7	Исследование свойств межсетевого экрана с пакетной фильтрацией	Ср.	4	ПК-10	Л3.2
1.8	Исследование свойств межсетевого экрана с сохранением состояний	Ср.	4	ПК-10	Л3.2
1.9	Исследование свойств межсетевого экрана ZBFW	ПЗ3	2	ПК-10	Л3.2
1.10	Требования нормативных документов и технических регламентов к защищенным сетям связи	Ср.	8	ПК-10	Л2.2 Л2.3
1.11	Технические характеристики аппаратных межсетевых экранов различных производителей	Ср.	8	ПК-10	Л1.1
1.12	Обеспечение защиты беспроводного сетевого оборудования	Ср.	6	ПК-10	Л1.1
1.13	Механизмы комплексной защиты сетей электросвязи	Ср.	6	ПК-10	Л1.1
Модуль 2 – Защита корпоративных сетей от НСД – 56 (6+50)часа					
2.1	Защита периметра корпоративной сети 1. Защита периметра с применением межсетевого экранирования 2. Статический NAT. 3. Динамический NAT. 4. NAT с применением маскарадинга	Лек.	2	ПК-10	Л1.1
2.2	Защита корпоративной информации, передаваемой по общедоступной сети 1. Определение и классификация VPN 2. Протоколы VPN, реализуемые на втором уровне модели OSI 3. Протоколы VPN, реализуемые на третьем уровне модели OSI 4. Протоколы туннелирования 5. Протоколы IPSec	Лек.	2	ПК-10	Л1.1
2.3	Конфигурирование NAT на маршрутизаторе	ПЗ4	2	ПК-10	Л3.1
2.4	Исследование VPN-туннеля	Ср.	10	ПК-10	Л3.2
2.9	Механизмы защиты корпоративной сети от DoS-атак	Ср.	10	ПК-10	Л1.1
2.10	Механизмы защиты корпоративной сети от компьютерных вирусов	Ср.	10	ПК-10	Л1.1
2.11	Области применения технологий VPN второго уровня	Ср.	10	ПК-10	Л1.1
2.12	Организационные мероприятия по комплексной защите корпоративной сети	Ср.	10	ПК-10	Л1.1
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Рекомендуемая литература				
5.1.2. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Манин А.А.	Методы и средства защиты компьютерной информации. Учебное пособие.	Ростов-на-Дону: СКФ МТУСИ, 2019.	Э1
5.1.2 Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Манин А.А.	Системы коммутации. Принципы и технологии пакетной коммутации. Учебное пособие.	Ростов-на-Дону: СКФ МТУСИ, 2014.	Э2
Л2.2	-	Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 “Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации”.		Э3
Л2.3	-	ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения		Э4
5.1.3 Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Манин А.А.	Методическое пособие для практических занятий по дисциплине «Методы и средства защиты компьютерной информации».	Ростов-на-Дону: СКФ МТУСИ, 2019.	Э5
Л3.2	Манин А.А.	Методическое пособие для лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации».	Ростов-на-Дону: СКФ МТУСИ, 2019.	Э6

6.2 Электронные образовательные ресурсы	
Э1	http://www.skf-mtusi.ru
Э2	http://www.skf-mtusi.ru/umo/110302st/48.2/L2.1%20Uchebnoe%20posobie.pdf
Э3	https://www.garant.ru/products/ipo/prime/doc/92632/
Э4	http://docs.cntd.ru/document/1200044726
Э5	http://www.skf-mtusi.ru
Э6	http://www.skf-mtusi.ru

6.3 Программное обеспечение	
П.1	ОС Windows
П.2	ОС Linux
П.3	Cisco Packet Tracer
П.4	ОС Cisco IOS
П.5	GNS-3

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерный класс с установленным пакетом Cisco Packet Tracer
2	Программно-аппаратный комплекс «Инфокоммуникационные сети»
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет.

7. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 7.1.

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Недел я	Кол. час.
Модуль 1			
1	**Требования нормативных документов и технических регламентов к защищенным сетям связи** 1.1. Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 1.2. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.	1-2	8

2	**Технические характеристики аппаратных межсетевых экранов различных производителей** 2.1 МСЭ Cisco. 2.2 МСЭ D-Link. 2.3 МСЭ Huawei. 2.4 МСЭ TP-link. 2.5 Отечественные решения.	3-4	8
3	**Обеспечение защиты беспроводного сетевого оборудования** 3.1. Процедуры аутентификации и авторизации в сетях IEEE 802.11. 3.2. Защита беспроводных устройств от НСД.	5-6	6
4	**Механизмы комплексной защиты сетей электросвязи** 4.1. Оформление политики безопасности сети. 4.2. Управление паролями. 4.3. Управление правами доступа. 4.4 Мониторинг активности пользователей. 4.5 Мониторинг уязвимости ПО. 4.6 Управление обновлениями ПО и ОС.	7-9	6
Модуль 2			
5	**Механизмы защиты корпоративной сети от DoS-атак** 7.1 Dos и DDos-атаки. 7.2 Системы обнаружения вторжений (IDS). 7.3 Системы предотвращения вторжений (IPS).	10-11	8
8	**Механизмы защиты корпоративной сети от компьютерных вирусов** 8.1 Классификация компьютерных вирусов. 8.2 Применение антивирусного ПО на шлюзах корпоративной сети. 8.3 Классификация корпоративного антивирусного ПО.	12-13	8
9	**Области применения технологий VPN второго уровня** 9.1 Протоколы PPTP, L2TP, L2PW. 9.2 Сравнительный анализ протоколов второго уровня. 9.3. Применение протоколов второго уровня в системе Site-to-Site. 9.4 Применение протоколов второго уровня в системе Remote VPN.	14-16	8
10	**Организационные мероприятия по комплексной защите корпоративной сети**	14-16	8

На самостоятельную работу студентам очно-заочной и заочной формы обучения выносится материал, представленный в таблице 9.2.

Таблица 9.2 – Учебный материал, выносимый на самостоятельное изучение студентам очно-заочной и заочной формы обучения

№№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	**Часы на изучение**
Модуль 1		
1	**Защита от несанкционированного доступа к сетевому оборудованию** 1.1 Защита консольного доступа 1.2 Протоколы удаленного доступа к оборудованию 1.3 Защита удаленного доступа	4
2	**Использование AAA-сервера для защиты удаленного доступа** 2.1 Протокол RADIUS 2.2 Протокол TACACS+	4 2
3	**Исследование свойств межсетевого экрана с пакетной**	4

	фильтрацией 3.1 Понятие списков доступа 3.2 Создание списков доступа и привязка их к интерфейсу	
4	**Исследование свойств межсетевого экрана с сохранением состояний** 4.1 Понятие МСЭ с сохранением состояний 4.2 Конфигурирование МСЭ	4
5	**Требования нормативных документов и технических регламентов к защищенным сетям связи** 5.1. Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 5.2. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.	8
6	**Технические характеристики аппаратных межсетевых экранов различных производителей** 6.1 МСЭ Cisco. 6.2 МСЭ D-Link. 6.3 МСЭ Huawei. 6.4 МСЭ TP-link. 6.5 Отечественные решения.	8
7	**Обеспечение защиты беспроводного сетевого оборудования** 7.1. Процедуры аутентификации и авторизации в сетях IEEE 802.11. 7.2. Защита беспроводных устройств от НСД.	6
8	**Механизмы комплексной защиты сетей электросвязи** 8.1. Оформление политики безопасности сети. 8.2. Управление паролями. 8.3. Управление правами доступа. 8.4 Мониторинг активности пользователей. 8.5 Мониторинг уязвимости ПО. 8.6 Управление обновлениями ПО и ОС.	6
Модуль 2		
9	**Механизмы защиты корпоративной сети от DoS-атак** 9.1 Dos и DDos-атаки. 9.2 Системы обнаружения вторжений (IDS). 9.3 Системы предотвращения вторжений (IPS).	10
10	**Механизмы защиты корпоративной сети от компьютерных вирусов** 10.1 Классификация компьютерных вирусов. 10.2 Применение антивирусного ПО на шлюзах корпоративной сети. 10.3 Классификация корпоративного антивирусного ПО.	10
11	**Области применения технологий VPN второго уровня** 10.1 Протоколы PPTP, L2TP, L2PW. 10.2 Сравнительный анализ протоколов второго уровня. 10.3. Применение протоколов второго уровня в системе Site-to-Site. 10.4 Применение протоколов второго уровня в системе Remote VPN.	10
12	**Организационные мероприятия по комплексной защите корпоративной сети**	10

Дополнения и изменения в Рабочей программе