

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.03 Основы информационной безопасности в
компьютерных сетях

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

09.04.01 Информатика и вычислительная техника

Направленность (профиль)

09.04.01.11 Вычислительные системы и сети

Форма обучения

очная

Год набора

2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

к.т.н., доцент, Казаков Федор Александрович

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Освоение методов разработки комплексной политики сетевой безопасности, настройки статических VPN соединений, конфигурирования устройств локальной сети

для контроля доступа, сопротивления атакам, защиты других сетевых устройств и систем, а также поддержки целостности и конфиденциальности сетевого трафика.

1.2 Задачи изучения дисциплины

Формирование у магистров навыков планирования и развертывания систем информационной безопасности в рамках построения корпоративных информационно-вычислительных сетей.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-3: Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению технических и программных средств вычислительной техники и сетевых решений	
ИД-1: Знать: особенности проведения совместных исследований по созданию (модификации) системного программного обеспечения и информационно-коммуникационной инфраструктуры, нормативно-технические документы (стандарты и регламенты), лучшие мировые практики и внутренние нормативные документы в части разработки требований на создание (модификацию) и сопровождение интеграционных, технических и программных средств вычислительной техники и сетевых решений, принципы и технологии функционирования выбранной платформы, методы и средства выявления дефектов, проблем и причин их возникновения.	основные принципы конфигурации сетевого оборудования

ИД-2: Уметь: уметь проводить анализ и систематизацию	выполнять конфигурацию системы безопасности
<p>знаний, сопутствующих разработке и сопровождению системного программного обеспечения и информационно-коммуникационной инфраструктуры, проектировать электрические схемы и системы тестирования логических элементов, в том числе на поведенческом языке, выполнять процедуры сборки программных модулей, сервисов и компонент в соответствии с техническим заданием с использованием целевых САПР, документировать произведенные действия, выявленные проблемы и способы их устранения, создавать инженерную документацию, унифицировать технические решения по разработке технических и программных средств вычислительной техники и сетевых решений</p>	
<p>ИД-3: Иметь навыки: разработки и анализа эффективности во время сопровождения системных и инструментальных программных средств, обеспечивающих сетевые и распределенные взаимодействия вычислительной техники, управления работами по проектированию и контролю подключения средств ВТ и интеграционных решений к компонентам внешней среды, тестирования и установления причин возникновения отклонений в различных режимах работы полученных решений.</p>	иметь навыки поддержки работоспособности сети

ПК-5: Способен управлять процессом проектирования, разрабатывать и применять на практике программное и аппаратное обеспечение для решения задач цифровой обработки сигналов	
ИД-1: Знать: знать методы исследования и анализа информационно-коммуникационных систем используемых для решения задач цифровой обработки сигналов, элементы теории сложных цифровых систем, общий маршрут процесса проектирования, методы и этапы проектирования, методы составления адекватных имитационных математических моделей ЭРИ в объеме выполняемой функции.	основные понятия информационной безопасности
ИД-2: Уметь: проводить анализ и проектирование информационно-коммуникационных систем используемых для решения задач цифровой обработки сигналов, управлять процессом проектирования, разрабатывать поведенческие модели и выполнять тестирование электронного оборудования.	разрабатывать политику информационной безопасности
ИД-3: Иметь навыки: проведения исследований и разработок информационно-коммуникационных систем используемых для решения задач цифровой обработки сигналов, автоматического синтеза, моделирования и проверки функционирования тестовой модели, анализа результатов моделирования и тестирования СФ-блоков, электронных средств и электронных систем, создания логической схемы, расчета параметров и режимов работы для аппаратуры цифровой обработки сигналов.	навыками управления информационной безопасностью

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: <https://e.sfu-kras.ru/course/view.php?id=11924>.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
Контактная работа с преподавателем:	1 (36)	
занятия лекционного типа	0,5 (18)	
лабораторные работы	0,5 (18)	
Самостоятельная работа обучающихся:	2 (72)	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
Промежуточная аттестация (Экзамен)	1 (36)	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

		Контактная работа, ак. час.							
№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Основы построения безопасной сети									
	1. Современные угрозы сетевой безопасности	0,5							
	2. Вирусы, черви и троянские кони	0,5							
	3. Методы и цели атак	0,5							
	4. Безопасный доступ к устройствам	0,5							
	5. Разработка примера политики информационной безопасности локальной сети. Настройка доступа к оборудованию с использованием шифрованного соединения на основе технологии сертификатов (ssh)					3			
	6. Освоение теоретического материала							6	
	7. Подготовка к выполнению лабораторных работ							2	
2. Реализация технологий фильтра пакетов									
	1. Технология фильтра пакетов	2							

2. Построение пакетных фильтров на основе списков (ACL)	2							
3. Установка и настройка граничного фильтра пакетов.					4			
4. Освоение теоретического материала							15	
5. Подготовка к лабораторным работам							4	
3. Реализация технологий безопасной виртуальной частной сети								
1. VPN технологии.	2							
2. Безопасность виртуальной частной сети.	2							
3. Установка и настройка виртуальной частной сети.					4			
4. Освоение теоретического материала							12	
5. Подготовка к лабораторным работам							7	
4. Безопасность локальной сети								
1. Безопасность точки подключения (конечной точки)	1							
2. Соображения безопасности второго уровня (Layer-2)	2							
3. Конфигурация безопасности второго уровня	2							
4. Конфигурирование системы безопасности второго уровня.					4			
5. Освоение теоретического материала							15	
6. Подготовка к лабораторным работам							3	
5. Управление безопасной сетью								
1. Принципы проектирования безопасной сети	2							
2. Проверка сетевой безопасности	1							
3. Разработка примера нормативного документа для контроля информационной безопасности корпоративной сети.					3			
4. Освоение теоретического материала							6	

5. Подготовка к лабораторным работам							2	
Всего	18				18		72	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем".(Москва: Питер).
2. Кузин А. В., Кузин Д. А. Компьютерные сети: Учебное пособие(Москва: Издательство "ФОРУМ").
3. Олифер В. Г., Олифер Н. А. Сетевые операционные системы: учебник для студентов вузов(Москва: Питер).
4. Джамалипур А. Беспроводной мобильный интернет : архитектура, протоколы и сервисы: пер. с англ.(Москва: Техносфера).
5. Жуков В. Г. Безопасность вычислительных сетей: Ч. 1. Базовые протоколы стека TCP/IP: учебное пособие для студентов, обучающихся по направлениям 090900.68, 230100.68 очной формы обучения (Красноярск: Сибирский аэрокосмический университет (СибГАУ)).
6. Таненбаум Э., Бос Х. Современные операционные системы(Москва: Питер).
7. Дибров М. В. Протоколы маршрутизации и передачи данных в Интернет: лаб. практикум для студентов спец. 230100.65, 230100.62, 230100.68(Красноярск: СФУ).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Putty - программа доступа по протоколу ssh

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Не требуется

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Компьютерный класс, оборудованный:

- 6-8 рабочими местами, позволяющими выполнять работу в парах как во время лекций, так и во время лабораторных работ;

- стендом в составе 6-и коммутаторов и 6-и маршрутизаторов;
- проекционным оборудование рабочего места преподавателя;
- маркерной доской.