МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное
бюджетное образовательное учреждение
высшего образования

«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

_____

«___»_____ 2024г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Информационная безопасность компьютерных сетей
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность (профиль):	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена на заседании кафедры математики и прикладных информационных технологий

Протокол №____от_____2024г.

1. Цели и задачи освоения дисциплины

1. Цель освоения дисциплины: владение теоретическими знаниями и умениями, развитие навыков практических действий по построению защищенных компьютерных сетей.

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ построения защищенных компьютерных сетей;
- изучение методов и процедур выявления угроз безопасности в компьютерных сетях и оценки степени их опасности;
- изучение методов построения защищенных компьютерных сетей;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях
- практическая отработка способов и порядка проведения работ по построению защищенных компьютерных сетей;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий и информационной безопасности;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины является логическим продолжением содержания дисциплины «Информационная безопасность компьютерных сетей» и может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать (З1) теоретические основы управления информационной безопасностью компьютерных систем и сетей
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения
		Владеть (В1) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения

		данных при сбоях
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	Знать (З2) теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения
		Уметь (У2) планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения
		Владеть (В2) практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать (З3) теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность
		Уметь (У3) планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения
		Владеть (В3) практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения
ПКС-4. Способен управлять процессами установки, конфигурирования и проводить регламентные работы на сетевых устройствах и программном обеспечении, а также обеспечивать и оптимизировать функционирование баз данных.	ПКС-4.1. Администрирует процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Знать (З4) теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных
		Уметь (У4) администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения
		Владеть (В4) практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных

4. Объем дисциплины

Общий объем дисциплины составляет 4 зачетных единиц, 144 часа.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/7	16	-	30	62	36	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Контроль, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.					
1	1	Правовые и организационные основы информационной безопасности	3	-	5	11	-	19	ПКС-1.1 ПКС-2.1 ПКС-3.1 ПКС-4.1	Задания на лабораторную работу
2	2	Технологии аутентификации, авторизации и управления доступом	3	-	6	12	-	21		
3	3	Технологии безопасности на основе анализа трафика	3	-	6	13	-	22		
4	4	Атаки на транспортную инфраструктуру сети	3	-	6	13	-	22		
5	5	Безопасность программного кода и сетевых служб	4	-	7	13	-	24		
6	Экзамен		-	-	-	-	36	36	ПКС-1.1 ПКС-2.1 ПКС-3.1 ПКС-4.1	Вопросы к экзамену
Итого:			16	-	30	62	36	144	X	X

заочная форма обучения (ЗФО): не реализуется

очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Правовые и организационные основы информационной безопасности. Основные понятия в области информационной безопасности. Нормативно-правовые акты, специаль-

ные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Модели информационной безопасности. Типы и примеры атак. Иерархия средств защиты. Принципы защиты информационной системы. Шифрование.

Раздел 2. Технологии аутентификации, авторизации и управления доступом. Технологии аутентификации. Технологии управления доступом и авторизации. Централизованные системы аутентификации и авторизации.

Раздел 3. Технологии безопасности на основе анализа трафика. Фильтрация. Файерволы. Прокси-серверы. Трансляция сетевых адресов. Системы мониторинга трафика. Аудит событий безопасности. Типовые архитектуры сетей, защищаемых файерволами.

Раздел 4. Атаки на транспортную инфраструктуру сети. Атаки на транспортные протоколы. Атаки на DNS. Безопасность маршрутизации на основе BGP. Технологии защищенного канала.

Раздел 5. Безопасность программного кода и сетевых служб. Уязвимости программного кода и вредоносные программы. Безопасность веб-сервиса. Безопасность электронной почты. Безопасность облачных сервисов.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	3	-	-	Правовые и организационные основы информационной безопасности
2	2	3	-	-	Технологии аутентификации, авторизации и управления доступом
3	3	3	-	-	Технологии безопасности на основе анализа трафика
4	4	3	-	-	Атаки на транспортную инфраструктуру сети
5	5	4	-	-	Безопасность программного кода и сетевых служб
Итого:		16	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Правовые и организационные основы информационной безопасности
2	2	6	-	-	Технологии аутентификации, авторизации и управления доступом
3	3	6	-	-	Технологии безопасности на основе анализа трафика
4	4	6	-	-	Атаки на транспортную инфраструктуру сети
5	5	7	-	-	Безопасность программного кода и сетевых служб
Итого:		30	-	-	-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	11	-	-	Правовые и организационные основы информационной безопасности	Подготовка к лабораторным работам, контрольная работа
2	2	12	-	-	Технологии аутентификации, авторизации и управления доступом	Подготовка к лабораторным работам, контрольная работа
3	3	13	-	-	Технологии безопасности на основе анализа трафика	Подготовка к лабораторным работам, контрольная работа
4	4	13	-	-	Атаки на транспортную инфраструктуру сети	Подготовка к лабораторным работам, контрольная работа
5	5	13	-	-	Безопасность программного кода и сетевых служб	Подготовка к лабораторным работам, контрольная работа
6	1-5	-	-	-	Экзамен	Подготовка к экзамену
Итого:		62	-	-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

– ИКТ – технологии (визуализация учебного материала в PowerPoint в диалоговом режиме);
– обучение в сотрудничестве (коллективная, групповая работа);
– технология проблемного обучения.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Лабораторная работа № 1	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	**0-30**
2 текущая аттестация		
3	Лабораторная работа № 3	0-15
4	Лабораторная работа № 4	0-15

	ИТОГО за вторую текущую аттестацию	**0-30**
3 текущая аттестация		
5	Лабораторная работа № 5	0-40
	ИТОГО за третью текущую аттестацию	**0-40**
	ВСЕГО	**0-100**

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;
- Электронно-библиотечная система «ЛАНЬ» https://e.lanbook.com;
- Образовательная платформа ЮРАЙТ www.urait.ru;
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;
- Библиотеки нефтяных вузов России:
  - Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/;
  - Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/;
  - Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- Nmap;
- Snort;
- Wireshark;
- OpenVPN.

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Информационная безопасность компьютерных сетей	Лекционные занятия: Учебная аудитория для проведения занятий лекционного	625039, г. Тюмень, ул. Мельникайте, д. 70.

		типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	
		Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.

В начале лабораторного занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания, подготовиться к научно-исследовательской деятельности. В процессе работы на лабораторных занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, изучение мультимедиалекций, расположенных в свободном доступе, решение ситуационных (профессиональных) задач, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: «Информационная безопасность компьютерных сетей»
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает	Знать (З1) теоретические основы управления информационной безопасностью компьютерных систем и сетей	Не знает теоретические основы управления информационной безопасностью компьютерных систем и сетей	Знает на низком уровне теоретические основы управления информационной безопасностью компьютерных систем и сетей	Знает на среднем уровне теоретические основы управления информационной безопасностью компьютерных систем и сетей	Знает в совершенстве теоретические основы управления информационной безопасностью компьютерных систем и сетей
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Не умеет планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на низком уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на среднем уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет в совершенстве планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
	безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Владеть (В1) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Не владеет практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет на низком уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет на среднем уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет в совершенстве практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программног	Знать (З2) теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Не знает теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Знает на низком уровне теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Знает на среднем уровне теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Знает в совершенстве теоретические основы администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
компьютерных системах и сетях.	о обеспечения.	Уметь (У2) планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения	Не умеет планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения	Умеет на низком уровне планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения	Умеет на среднем уровне планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения	Умеет в совершенстве планировать и организовывать мероприятия по техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения
		Владеть (В2) практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Не владеет практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Владеет на низком уровне практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Владеет на среднем уровне практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения	Владеет в совершенстве практическими навыками внедрения, настройки, администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях, средств защиты информации прикладного и системного программного обеспечения

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать (ЗЗ) теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность	Не знает теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность	Знает на низком уровне теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность	Знает на среднем уровне теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность	Знает в совершенстве теоретические основы проведения аудита компьютерных систем и сетей и программного обеспечения на защищенность
		Уметь (УЗ) планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения	Не умеет планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения	Умеет на низком уровне планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения	Умеет на среднем уровне планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения	Умеет в совершенстве планировать и организовывать мероприятия по аудиту компьютерных систем и сетей и программного обеспечения на защищенность, разрабатывать тестовые случаи для программного обеспечения
		Владеть (В3) практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения	Не владеет практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения	Владеет на низком уровне практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения	Владеет на среднем уровне практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения	Владеет в совершенстве практическими навыками оценки уровня безопасности компьютерных систем и сетей; тестирования программного обеспечения

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-4. Способен управлять процессами установки, конфигурирования и проводить регламентные работы на сетевых устройствах и программном обеспечении, а также обеспечивать и оптимизировать функционирование баз данных.	ПКС-4.1. Администрирует процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Знать (З4) теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных	Не знает теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных	Знает на низком уровне теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных	Знает на среднем уровне теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных	Знает в совершенстве теоретические основы внедрения, настройки и конфигурирования сетевых устройств и программного обеспечения, функционирования и оптимизации баз данных
		Уметь (У4) администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения	Не умеет администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения	Умеет на низком уровне администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения	Умеет на среднем уровне администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения	Умеет в совершенстве администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения
		Владеть (В4) практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных	Не владеет практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных	Владеет на низком уровне практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных	Владеет на среднем уровне практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных	Владеет в совершенстве практическими навыками внедрения, настройки, администрирования и конфигурирования сетевых устройств, программного обеспечения и баз данных

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: «Информационная безопасность компьютерных сетей»
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449285	ЭР*	30	100	+
2	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739	ЭР*	30	100	+

ЭР* – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/

Лист согласования 00ДО-0000758577

Внутренний документ "Информационная безопасность компьютерных сетей_2024_ИБКСб_09.03.01"

Ответственный: Кармацкая Елена Александровна

Согласовано

Серийный номер ЭП	Должность	ФИО	ИО	Виза	Комментарий	Дата
	Заведующий кафедрой, имеющий ученую степень доктора наук	Барбаков Олег Михайлович		Согласовано		
	Директор	Каюкова Дарья Хрисановна		Согласовано	Отредактировано	
	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		