МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Заведующий кафедрой
Интеллектуальных систем и технологий

_____О.Ф. Данилов
«__» _____ 2024 г

РАБОЧАЯ ПРОГРАММА

дисциплины: **Информационная безопасность и защита информации**

направление подготовки: **09.03.02 Информационные системы и технологии**

направленность: **Информационные системы и технологии в геологии и нефтегазовой отрасли**

форма обучения: **очная, заочная**

Рабочая программа рассмотрена на заседании кафедры Интеллектуальных систем и технологий для направления 09.03.02 Информационные системы и технологии (профиль) «Информационные системы и технологии в геологии и нефтегазовой отрасли»

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины – изучение теоретических основ информационной безопасности, основных принципов, методов и средств защиты информации в процессе ееобработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

- знакомство с сетевыми угрозами;
- изучение технологий межсетевого экрана;
- знакомство со средствами обеспечения безопасности локальной сети
- изучение криптографических систем;
- знакомство с технологиями VPN

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

знания: способов и средств защиты информации от утечки по техническим каналам иконтроля эффективности защиты информации;;

умения: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;

владения: методами и средствами технической защиты информации; методами расчета иинструментального контроля показателей технической защиты информации.

Содержание дисциплины является логическим продолжением таких дисциплин, как

«Операционные системы» и «Инфокоммуникационные системы и сети».

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине (модулю)
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	З1 Знать: виды ресурсов и ограничений для решения профессиональных задач;основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
		У1 Уметь: формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта
		В1 Владеть: навыком постановки задач, необходимых для достижения цели проекта
ПКС-5 Способность выполнять работы по обеспе-	ПКС-5.1 Анализирует программные сред-	З2 Знать: программные средства управления базами дан-

чению функционирования баз данных и обеспечению их информационной безопасности	ства управления базами данных; угрозы и средства защиты их информационной безопасности	ных, виды угроз и средства защиты их информационной безопасности
	ПКС-5.2 Выполняет администрирование баз данных и обеспечение их информационной безопасности	У2 Уметь: применять методы и технологии обеспечения информационной безопасности баз данных

4. Объем дисциплины

Общий объем дисциплины составляет 4 зачетных единицы, 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	28	-	28	52	36	экзамен
заочная	5/9	10	-	16	109	9	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.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1.	Введение в информационную безопасность.	1		2	3	6	УК-2.1	Задания для лабораторных работ, написание реферата, коллоквиум
2	2.	Правовое обеспечение информационной безопасности	1		2	3	6	УК-2.1	Задания для лабораторных работ, написание реферата, коллоквиум
3	3.	Организационное обеспечение информационной безопасности	1		2	3	6	УК-2.1	Задания для лабораторных работ, написание реферата, коллоквиум
4	4.	Технические средства обеспечения информационной безопасности.	3		2	3	8	ПКС-5.1	Задания для лабораторных работ, написание реферата, коллоквиум
5	5.	Система Предотвращения вторжений IPS.	2		2	3	7	ПКС-5.2	Задания для лабораторных работ, написание реферата, коллоквиум

6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защитапрограммных средств.	3		2	3	8	ПКС-5.2	Задания для лабораторных работ, написание реферата, коллоквиум
7	7.	Защита от компьютерных вирусов	3		2	3	8	ПКС-5.2	Задания для лабораторных работ, написание реферата, коллоквиум
8	8.	Криптографические системы.	2		2	4	8	ПКС-5.2	Задания для лабораторных работ, написание реферата, коллоквиум
9	9.	Обеспечение безопасности локальной сети.	2		2	4	8	УК-2.1	Задания для лабораторных работ, написание реферата, тестирование
10	10.	Защита от потериинформации и отказов программно-аппаратных средств.	2		2	4	8	УК-2.1	Задания для лабораторных работ, написание реферата, тестирование
11	11.	Защита информационно-программного обеспечения на уровне операционных систем.	2		2	4	8	ПКС-5.2	Задания для лабораторных работ, тестирование
12	12.	Виртуальные частные сети VPN	2		2	5	9	ПКС-5.1	Задания для лабораторных работ, написание реферата, тестирование
13	13.	Специфические особенности защиты информации влокальных и глобальных компьютерных сетях.	2		2	5	9	УК-2.1	Задания для лабораторных работ, написание реферата, тестирование
14	14.	Управление безопасной сетью.	2		2	5	9	УК-2.1	Задания для лабораторных работ, написание реферата, тестирование
15	15.	Экзамен	-	-	-	36	36	УК-2.1 ПКС-5.1 ПКС-5.2	вопросы к экзамену
Итого:			28		28	52	144		

Заочная форма обучения (ОФО)

Таблица 5.2

№ п/п	Структура	Аудиторные занятия, час.	СРС,	Всего, час.	Код ИДК	Оценочные средства

	дисциплины					час.			
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1.	Введение в информационную безопасность.	1		1	6	7	УК-2.1	Задания для лабораторных работ, контрольная работа, коллоквиум
2	2.	Правовое обеспечение информационной безопасности			1	9	10	УК-2.1	Задания для лабораторных работ, контрольная работа, коллоквиум
3	3.	Организационное обеспечение информационной безопасности			1	6	8	УК-2.1	Задания для лабораторных работ, контрольная работа, коллоквиум
4	4.	Технические средства обеспечения информационной безопасности.	1		1	8	9	ПКС-5.1	Задания для лабораторных работ, контрольная работа, коллоквиум
5	5.	Система Предотвращения вторжений IPS.			1	8	9	ПКС-5.2	Задания для лабораторных работ, контрольная работа, коллоквиум
6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защитапрограммных средств.			2	8	11	ПКС-5.2	Задания для лабораторных работ, контрольная работа, коллоквиум
7	7.	Защита от компьютерных вирусов	1		1	8	10	ПКС-5.2	Задания для лабораторных работ, контрольная работа, коллоквиум
8	8.	Криптографические системы.	2		1	8	11	ПКС-5.2	Задания для лабораторных работ, контрольная работа, коллоквиум
9	9.	Обеспечение безопасности локальной сети.	1		1	8	9	УК-2.1	Задания для лабораторных работ, контрольная работа, тестирование
10	10.	Защита от потериинформации и отказов программно-аппаратных средств.			1	8	10	УК-2.1	Задания для лабораторных работ, контрольная работа, тестирование
11	11.	Защита информационно-программного обеспечения на уровне операционных систем.	2		1	8	11	ПКС-5.2	Задания для лабораторных работ, контрольная работа, тестирование
12	12.	Виртуальные частные сети VPN	2		1	8	9	ПКС-5.1	Задания для лабораторных работ, контрольная

									работа, тестирование
13	13.	Специфические особенности защиты информации влокальных и глобальных компьютерных сетях.			1	8	9	УК-2.1	Задания для лабораторных работ, контрольная работа, тестирование
14	14.	Управление безопасной сетью.			2	8	12	УК-2.1	Задания для лабораторных работ, контрольная работа, тестирование
15	15.	Экзамен	-	-	-	9	9	УК-2.1 ПКС-5.1 ПКС-5.2	Вопросы экзамена
Итого:			10		16	118	144		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение в информационнуюбезопасность.	Угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ.
2.	Правовое обеспечение информационной безопасности	Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации
3.	Организационное обеспечение информационной безопасности	Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.
4.	Технические средства обеспечения информационнойбезопасности.	Общие вопросы организации противодействия сетевым атакам; аппаратураконтроля.
5.	Система предотвращениявторжений IPS.	Технологии IPS. Сигнатуры IPS (набор правил обнаружения вторжений),характеристики, сигналы и действия сигнатур.

6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Способы разграничения доступа к компьютерным ресурсам. Понятие меток безопасности. Защита программных средств от несанкционированного копирования, исследования и модификации.
7.	Защита от компьютерных вирусов.	Классификация компьютерных вирусов. Общая организация защиты откомпьютерных вирусов. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Использование средств аппаратного и программногоконтроля.
8.	Криптографическиесистемы.	Введение в криптографию. Защита обмена данными. Криптография. Криптоанализ. Криптология. Простые методы шифрования: шифры подстановки и перестановки. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации.
9.	Обеспечение безопасности локальнойсети.	Безопасность оконечных устройств. Защита от вредоносного ПО. Защита электронной почты и Web-трафика. Управление доступом к сети. Нейтрализация атак на DHCP, ARP и сеть VLAN.
10.	Защита от потери информации и отказов программно-аппаратных средств.	Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Способы резервировании информации. Подготовка программных средств восстановления. Восстановление и оптимизация оперативной памяти компьютера.
11.	Защита информационно-программного обеспечения на уровне операционных систем.	Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Подсистемы безопасности современных ОС (Windows, UNIX), их недостатки и основные направления совершенствования.
12.	Виртуальные частные сети VPN	Топологии сетей VPN. Реализация сетей VPN.
13.	Специфические особенности защитыинформации в локальных и глобальных компьютерных сетях.	Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды.. Защита в Internet и Intranet. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов.
14.	Управление безопаснойсетью	Тестирование безопасности сети: методика и инструменты. Разработка комплексной политики безопасности: структура политики безопасности,стандарты, правила и процедуры, реагирование на нарушение безопасности.

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	1	1	0	Введение в информационнуюбезопасность.
2	2	1		0	Правовое обеспечение информационной безопасности
3	3	1		0	Организационное обеспечение информационной безопасности
4	4	3	1	0	Технические средстваобеспечения информационнойбезопасности.
5	5	2		0	Система предотвращениявторжений IPS.
6	6	3		0	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.

7	7	3	1	0	Защита от компьютерных вирусов.
8	8	2	2	0	Криптографическиесистемы.
9	9	2	1	0	Обеспечение безопасности локальнойсети.
10	10	2		0	Защита от потери информации и отказов программно-аппаратных средств.
11	11	2	2	0	Защита информационно-программного обеспечения на уровне операционных систем.
12	12	2	2	0	Виртуальные частные сети VPN
13	13	2		0	Специфические особенности защитыинформации в локальных и глобальных компьютерных сетях.
14	14	2		0	Управление безопаснойсетью
Итого:		28	10	0	

Практические занятия

Практические занятия учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	3, 14	3	2	0	Управление безопасностью сети.
2	4, 12, 13	3	2	0	Обеспечение безопасности сетевых устройств.
3	5, 1,2,3	3	2	0	Аутентификация, авторизация и учет.
4	6	3	2	0	Внедрение технологий межсетевого экрана.
5	9	3	2	0	Обеспечение безопасности локальной сети.
6	7, 11	4	2	0	Анализ способов нарушений информационной безопасности.
7	9,3	4	2	0	Основные технологии построения защищенных систем.
8	8	5	2	0	Методы криптографии. .
Итого:		28	16	0	

Самостоятельная работа студента

Таблица 5.2.3

№п/п	Номер раздела-дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	3	6		Методологические и технологические основыкомплексного обеспечения ИБ;модели, стратегии и системы обеспечения ИБ; правовые инормативные акты в области ИБ.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
2	2	3	6		Распределение доступа в локальных сетях сиспользованием ACL.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
3	3	3	6		Инструменты хакера. Вредоносное ПО.Распространенные сетевые атаки.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы

4	4	3	6		Технологии IPS. Сигнатуры IPS(набор правил обнаружения вторжений), характеристики, сигналы и действия сигнатур.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
5	5	3	6		Функции ядра системыкомплексной защиты. Многоуровневая структура системы защиты на основепрограммно-аппаратных средстввычислительной системы. Стандарты по оценкебезопасности вычислительныхсистем.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
6	6	3	6		Безопасность оконечных устройств. Защита отвредоносного ПО. Защита электронной почты и Web- трафика. Управление доступом к сети. Нейтрализация атак наDHCP, ARP и сеть VLAN.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
7	7	3	6		Стандарт шифрования данных.Криптография открытых ключей.Цифровыеподписи. Инфраструктура открытыхключей.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
8	8	4	6		Режимы шифрования. Особенности шифрованияданных в режиме реального времени.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы
9	9	4	6		Топологии сетей VPN.Реализация сетей VPN.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы, подготовка к тестированию
10	10	4	6		Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физическихдефектов магнитных дисков. Восстановление разметки.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы, подготовка к тестированию
11	11	4	6		Аппаратная основа реализациизащиты на уровне ОС. Стандарты по оценке уровня безпасности ОС.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы, подготовка к тестированию
12	12	5	6		Тестирование безопасности сети: методика и инструменты. Разработка комплексной политики безопасности:структура политики безопасности,стандарты, правила и процедуры, реагирование на нарушение безопасности	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы, подготовка к тестированию
13	13	5	6		Защита в Internet и Intranet.	Подготовка к лабораторной работе, написание реферата, выполнение контрольной работы, подготовка к тестированию

14	14	5	6		Понятие изолированнойпрограммной среды, защита программ от изменения и контроль целостности;системные вопросы защитыпрограмм и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно- аппаратные средстваобеспечения информационной безопасности в типовыхоперационных системах, системах управлениябазами данных, вычислительных сетях.	Подготовка к лабораторной работе
	Экзамен	36	9			Подготовка к экзамену
Итого:		88	118			

5.2.3. Преподавание дисциплины ведется с применением следующих видовобразовательных технологий:

- решение задач, выполнение практических заданий, проектов (лабораторные занятия);
- работа в малых группах (лабораторные занятия);
- разбор практических ситуаций (лекционные занятия).

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы *(для заочной формы обучения)*

7.1. Методические указания для выполнения контрольных работ.

Контрольные работы выполняются самостоятельно в период между сессиями по индивидуальным заданиям. Тематика заданий определяется преподавателем, соответствует разделам дисциплины и сообщается обучающимся не позже, чем за две недели до начала зимней сессии 5 курса. Во время сессии обучающийся должен сдать преподавателю в печатном виде отчет по контрольной работе и устно защитить его.

7.2. Тематика контрольных работ.

Основные темы контрольных работ:

1. Защита интеллектуальной собственности средствами патентного и авторского права.
2. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения.
3. Стандарты по оценке безопасности вычислительных систем.
4. Защита программных средств от несанкционированного копирования, исследования и модификации.
5. Стратегия подготовки к ликвидации последствий вирусной эпидемии.
6. Режимы и средства шифрования.
7. Технология восстановления дисковой и оперативной памяти.
8. Аппаратная основа реализации защиты на уровне ОС.
9. Методы управления параллельными транзакциями.
10. Инструментальные средства СУБД по обеспечению целостности баз данных.
11. Защита программ от изменения и контроль целостности.

12. Программно-аппаратные средства обеспечения информационной безопасности в операционных системах, системах управления базами данных, вычислительных сетях.

8. Оценка результатов освоения дисциплины/модуля

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 представлена ниже.

Таблица 8.1

№	Виды контрольных мероприятий	Баллы
1	Выполнение лабораторных работ	0-20
2	Коллоквиум	0-20
	Итого за I аттестацию	**0-40**
3	Выполнение лабораторных работ	0-20
4	Защита реферата	0-20
5	Тестирование	0-20
	Итого за II аттестацию	**0-60**
	ВСЕГО	**100**

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

Таблица 8.2

№	Виды контрольных мероприятий	Баллы
1	Выполнение лабораторных работ	0-40
2	Коллоквиум	0-20
3	Защита отчета по контрольной работе	0-20
4	Тестирование	0-20
	ВСЕГО	**100**

8. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочныесистемы:

1. Библиотека академии наук – http://www.neva.ru/
2. Издательство «Открытые системы» - http://www.osp.ru/;
3. Центр информационных технологий МГУ - http://www.citforum.ru;
4. Регистрационно-информационная служба InterNIC - http://www.internic.net/;
5. Сервер телеконференций РАН - news://ipsun.ras.ru/;
6. Российский НИИ Информационных Систем - http://www.riis.ru;
7. Российский Институт Общественных Сетей - http://www.ripn.net;
8. Корпорация «Университетские сети знаний» UNICOR - http://www.rc.ac.ru.
9. Библиотека учебников, руководств и текстов по программированию -http://www.codenet.ru/

10. Upgrade: компьютерный еженедельник / Издательский Дом «Венето». Режим доступа:http://www.upweek.ru/

11. Компьютер БИЛД: европейский журнал о компьютерах / ИД «Бурда». Режим доступа: -http://www.computerbild.ru/

12. Издательство «Открытые системы»: портал издательства «Открытые системы». Режимдоступа: http://www.osp.ru/

13. База данных о предприятиях, анализа СМИ в разрезе контрагента http://www.integrum.ru/

14. Законодательство связанное с Интернет-деятельностью и информационнойбезопасностью http://www.internet-law.ru/

15. Методические пособия связанные с информационной безопасностью: http://all-ib.ru/

16. Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/

17. Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/

18. Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru

19. Электронно-библиотечная система «Лань» https://e.lanbook.com

20. Образовательная платформа ЮРАЙТ www.urait.ru

21. Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru

22. Национальная электронная библиотека (НЭБ)

23. 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

Oracle VM VirtualBox

Microsoft Windows

Cisco Packet Tracer

10. Материально-техническое обеспечение дисциплины/модуля

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

Таблица 10.1

№ п/п	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы	Перечень основного оборудования, учебно-наглядных пособий
1	Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации	Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 1 шт., проектор – 1 шт., проекционный экран – 1 шт., акустическая система (колонки) -2 шт., микрофон - 1 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.4

2	Помещение для самостоятельной работы обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду	Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 5 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.2, корп.1

11. Методические указания по организации СРС

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения, подготовке отчетов по лабораторным работам и подготовке к коллоквиумам. Преподаватель на занятии дает рекомендации необходимые для освоения материала. В ходе самостоятельной работы обучающиеся должны работать с информацией в сети Интернетом и учебной литературой. Обучающиеся должны понимать содержание выполненной работы (знать определения основных понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п.).

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **09.03.02 Информационные системы и технологии**
Направленность: **Информационные системы и технологии в геологии и нефтегазовой отрасли**

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	З1Знать: виды ресурсов и ограничений для решения профессиональных задач;основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Не освоил видыресурсов и ограничений длярешения профессиональн ых задач; основные методы оценки разных способоврешения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Частично освоилвиды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решениязадач; действующее законодательствои правовые нормы, регулирующие профессиональную деятельность	В основном освоил видыресурсов и ограничениядля решения профессиональных задач; основные методы оценкиразных способов решения задач;действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Полноценноосвоил видыресурсов и ограничениядля решения профессиональных задач; основные методы оценкиразных способов решения задач;действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
		У1 Уметь: формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта	Не умеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта	Частично умеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта	В основномумеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта	Полноценноумеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта

		В1Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	Не владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно- правовой документацией	Частично владеетметодиками разработки цели изадач проекта; методами оценкипотребности в ресурсах, продолжительности и стоимости проекта; навыкамиработы с нормативно-правовой документацией	В основномвладеет методикамиразработки цели и задачпроекта; методамиоценки потребности вресурсах, продолжительности и стоимостипроекта; навыкамиработы с нормативно-правовой документацией	Полноценновладеет методикамиразработки цели и задачпроекта; методамиоценки потребности вресурсах, продолжительности и стоимостипроекта; навыкамиработы с нормативно-правовой документацией
ПКС-5 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-5.1 Анализирует программные средства управления базами данных; угрозы и средства защиты их информационной безопасности	З2 Знать: программные средства управления базами данных, виды угроз и средства защиты их информационной безопасности	Не знает программные средства управления базами данных, виды угроз и средства защиты их информационной безопасности	Знает отдельные программные средства управления базами данных, виды угроз и средства защиты их информационной безопасности	Знает основные программные средства управления базами данных, виды угроз и средства защиты их информационной безопасности	Знает наиболее современные и эффективные программные средства управления базами данных, виды угроз и средства защиты их информационной безопасности
	ПКС-5.2 Выполняет администрирование баз данных и обеспечение их информационной безопасности	У2 Уметь: применять методы и технологии обеспечения информационной безопасности баз данных	Не умеет применять методы и технологии обеспечения информационной безопасности баз данных	Умеет частично применять методы и технологии обеспечения информационной безопасности баз данных	Умеет применять наиболее распространенные методы и технологии обеспечения информационной безопасности баз данных	Умеет применять наиболее современные и эффективные методы и технологии обеспечения информационной безопасности баз данных

Приложение 2

КАРТА
обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина Информационная безопасность и защита информации
Код, направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) Информационные системы и технологии в геологии и нефтегазовой отрасли

№ 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	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 c. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87992.html	ЭР*	30	100	+
2	Комплексное обеспечение информационной безопасности автоматизированных систем : учебное пособие / составители М. А. Лапина [и др.]. — Ставрополь : СКФУ, 2016. — 242 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155111	ЭР*	30	100	+
3	Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 c. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10677.html	ЭР*	30	100	+

4	Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html	ЭР*	30	100	+

*ЭР – электронный ресурс доступный через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/