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

УТВЕРЖДАЮ:
Председатель КСН
О.Н. Кузяков
«4» сентября 2019г.

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**

Рабочая программа разработана в соответствии с утвержденным учебным планом от 22 апреля 2019г. и требованиями ОПОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии, направленность Информационные системы и технологии в геологии и нефтегазовой отрасли к результатам освоения дисциплины «Информационная безопасность и защита информации».

Рабочая программа рассмотрена
на заседании Прикладной геофизики

Протокол № __1___ от «_3__» _сентября__ 2019 г.

Заведующий кафедрой _____ С.К. Туренко

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой_____ С.К. Туренко

«3» сентября 2019 г.

Рабочую программу разработал:

Вяткин А.И., доцент кафедры ПГФ ИГиН ТИУ,
к.т.н., доцент _____

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины – изучение теоретических основ информационной безопасности, основных принципов, методов и средств защиты информации в процессе ее обработки, 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.

Содержание дисциплины является логическим продолжением таких дисциплин, как «Операционные системы» и «Инфокоммуникационные системы и сети».

Содержание дисциплины служит основой для освоения дисциплин «Надежность и качество информационных систем», «Корпоративные информационные системы» и будет полезна для выполнения выпускной квалификационной работы.

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.З2 Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.	З1 виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
	УК-2.У2 Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.	У1 проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности
	УК-2.В2 Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах,	В1 методиками разработки цели и задач проекта; методами оценки потребности в ресурсах,

	продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией.	продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией
ПКС-2 Способность проводить исследования на всех этапах жизненного цикла программных средств, автоматизирующих задачи организационного управления и бизнес-процессы в геологии и нефтегазовой отрасли	ПКС-2.З2 Знать: основные модели и методы информационных систем и технологий в геологии и нефтегазовой отрасли	З2 Знать языки программирования, используемые при решении задач вычислительной математики
	ПКС-2.У2 Уметь: Проводить исследование моделей и методов информационных систем и технологий в геологии и нефтегазовой отрасли	У2 Уметь решать типовые задачи вычислительной математики с применением методов программирования
	ПКС-2.В2 Владеть: навыками анализа и моделирования информационных процессов и систем в геологии и нефтегазовой отрасли	В2 Владеть навыками решения задач профессиональной деятельности с использованием современных языков программирования

4. Объем дисциплины

Общий объем дисциплины составляет 5 зачетных единицы, 180 часа.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
очная	4/7	28	-	28	124	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.	Из них в интерактивной форме обучения, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.					
1	1.	Введение в информационную безопасность.	0		2	8	12	1	УК-2.З2	Вопросы и задания для коллоквиума, Вопросы экзамена, Задания для лабораторных работ
2	2.	Сетевые угрозы	0		2	8	12	1	УК-2.У2	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
3	3.	Внедрение	3		2	8	12		УК-2.В2	Вопросы

		технологий межсетевого экрана.								коллоквиума, Вопросы экзамена, Задания для лабораторных работ Задания для самостоятельной работы
4	4.	Технические средства обеспечения информационной безопасности.	3		2	8	12	1	ПКС-2.З2	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
5	5.	Система предотвращения вторжений IPS.	3		2	8	12		ПКС-2.У2	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	3		2	9	13	1	ПКС-2.У2	Вопросы коллоквиума, Вопросы экзамена, Задания для самостоятельной работы
7	7.	Защита от компьютерных вирусов.	3		2	9	13		ПКС-2.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
8	8.	Криптографические системы.	4		2	9	13	1	ПКС-2.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
9	9.	Обеспечение безопасности локальной сети.	4		2	9	13		УК-2.В2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
10	10.	Защита от потери информации и отказов программно-аппаратных средств.	5		2	9	13	1	УК-2.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
11	11.	Защита информационно-программного	0		2	9	13		ПКС-2.У2	Вопросы экзамена, Вопросы

		обеспечения на уровне операционных систем.								экзамена, Задания для самостоятельной работы
12	12.	Виртуальные частные сети VPN	0		2	10	14	1	ПКС-2.32	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
13	13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	0		2	10	14	1	УК-2.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
14	14.	Управление безопасной сетью.	0		2	10	14	1	УК-2.В2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
Итого:			28		28	124	180	9		

-

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).

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение в информационную безопасность.	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.	Сетевые угрозы	Инструменты хакера. Вредоносное ПО. Распространенные сетевые атаки.
3.	Внедрение технологий межсетевого экрана	Списки контроля доступа ACL. Нейтрализация атак с помощью ACL. Технологии межсетевого экрана.
4.	Технические средства обеспечения информационной безопасности.	Общие вопросы организации противодействия сетевым атакам; аппаратура контроля.
5.	Система предотвращения вторжений IPS.	Технологии IPS. Сигнатуры IPS (набор правил обнаружения вторжений), характеристики, сигналы и действия сигнатур.
6.	Предотвращение несанкционированного доступа к компьютерным	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

	ресурсам и защита программных средств.	несанкционированного копирования, исследования и модификации.
7.	Защита от компьютерных вирусов.	Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Использование средств аппаратного и программного контроля.
8.	Криптографические системы..	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 локальной сети.	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 защиты информации 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 безопасной сетью	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	2	0	0	Введение в информационную безопасность.
2	2	2	0	0	Сетевые угрозы
3	3	2	0	0	Внедрение технологий межсетевого экрана
4	4	2	0	0	Технические средства обеспечения информационной безопасности.
5	5	2	0	0	Система предотвращения вторжений IPS.
6	6	2	0	0	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
7	7	2	0	0	Защита от компьютерных вирусов.
8	8	2	0	0	Криптографические системы..
9	9	2	0	0	Обеспечение безопасности локальной сети.
10	10	2	0	0	Защита от потери информации и отказов программно-аппаратных средств.
11	11	2	0	0	Защита информационно-программного обеспечения на уровне

					операционных систем.
12	12	2	0	0	Виртуальные частные сети VPN
13	13	2	0	0	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.
14	14	2	0	0	Управление безопасной сетью
Итого:		28	0	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	3	0	0	Управление безопасностью сети.
2	4	3	0	0	Обеспечение безопасности сетевых устройств.
3	5	3	0	0	Аутентификация, авторизация и учет.
4	6	3	0	0	Внедрение технологий межсетевого экрана.
5	7	3	0	0	Обеспечение безопасности локальной сети.
6	8	4	0	0	Анализ способов нарушений информационной безопасности..
7	9	4	0	0	Основные технологии построения защищенных систем.
8	10	5	0	0	Методы криптографии. .
Итого:		28	0	0	

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	8	0	0	Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; правовые и нормативные акты в области ИБ.	Отчет по выполнению самостоятельной работы
2	2	8	0	0	Распределение доступа в локальных сетях с использованием ACL.	Отчет по выполнению самостоятельной работы
3	3	8	0	0	Инструменты хакера. Вредоносное ПО. Распространенные сетевые атаки.	Отчет по выполнению самостоятельной работы
4	4	8	0	0	Технологии IPS. Сигнатуры IPS (набор правил обнаружения вторжений), характеристики, сигналы и действия сигнатур. .	Отчет по выполнению самостоятельной работы
5	5	8			Функции ядра системы комплексной защиты.	Отчет по выполнению самостоятельной работы

					Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем.	
6	6	9			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.	Отчет по выполнению самостоятельной работы
7	7	9			Стандарт шифрования данных. Криптография открытых ключей. Цифровые подписи. Инфраструктура открытых ключей.	Отчет по выполнению самостоятельной работы
8	8	9			Режимы шифрования. Особенности шифрования данных в режиме реального времени.	Отчет по выполнению самостоятельной работы
9	9	9			Топологии сетей VPN. Реализация сетей VPN.	Отчет по выполнению самостоятельной работы
10	10	9			Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога	Отчет по выполнению самостоятельной работы
11	11	9			Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС.	Отчет по выполнению самостоятельной работы
12	12	10			Тестирование безопасности сети: методика и инструменты. Разработка комплексной политики безопасности: структура политики безопасности, стандарты, правила и процедуры, реагирование на нарушение безопасности	Отчет по выполнению самостоятельной работы
13	13	10			Защита в Internet и Intranet.	Отчет по выполнению самостоятельной работы
14	14	10			Понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной	Отчет по выполнению самостоятельной работы

					безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.	
Итого:		124	0	0		

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

решение задач, выполнение практических заданий, проектов (практические занятия);

– работа в малых группах (практические занятия);

– разбор практических ситуаций (лекционные занятия).

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

№	Виды контрольных мероприятий	Баллы	№ недели
1	Работа на лабораторных занятиях	0-10	1-5
2	Тест по теоретическому курсу: «Списки контроля доступа ACL»	0-15	5
3	Коллоквиум по СРС	0-5	4
	ИТОГО	**30**	
4	Работа на лабораторных занятиях	0-10	6-10
5	Тест по теоретическому курсу: «Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Защита от компьютерных вирусов. Криптографическое закрытие информации. Уничтожение остаточных данных.».	0-15	10
6	Коллоквиум по СРС	0-5	9
	ИТОГО	**30**	
7	Работа на лабораторных занятиях	0-15	11-17
8	Тест по теоретическому курсу: «Защита от потери информации и	0-15	17

	отказов программно-аппаратных средств. Защита информационно-программного обеспечения на уровне операционных систем. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях. Современные средства защиты информации от НСД.».		
9	Коллоквиум по СРС	0-10	16
	ВСЕГО	**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:

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». Режим доступа: 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 информационной безопасностью http://www.internet-law.ru/
15. Методические пособия связанные с информационной безопасностью: http://all-ib.ru/

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

1. Microsoft Office Professional Plus;
2. Windows Server 2012

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	Перечень оборудования,	Перечень технических средств обучения,

	необходимого для освоения дисциплины/модуля	необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
1	Персональные компьютеры	Комплект мультимедийного оборудования: проектор, экран, компьютер, акустическая система. Локальная и корпоративная сеть

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям

Порядок подготовки к лабораторным занятиям изложен в следующем учебно-методическом пособии:

Информационная безопасность и защита информации: методические указания для лабораторных и самостоятельных работ студентов, обучающихся по направлению 09.03.02 «Информационные системы и технологии» / сост. А.А. Яйлеткан: Тюменский индустриальный университет. – 1-е изд.– Тюмень: Издательский центр БИК, ТИУ, 2016. – 21 с.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в подготовке отчетов по лабораторным работам, подготовке к коллоквиумам.

Преподаватель на занятии дает рекомендации, необходимые для выполнения заданий.

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 и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
УК-2.	З1 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 виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Частично освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	В основном освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Полноценно освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
	У1 проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Не умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Частично проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	В основном умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Полноценно умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности

	В1 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 владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	В основном владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	Полноценно владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией
ПКС-2	З2 Знать языки программирования, используемые при решении задач вычислительной математики	Не знает языки программирования, используемые при решении задач вычислительной математики	Демонстрирует знание отдельных понятий языков программирования, используемых при решении задач вычислительной математики	Демонстрирует достаточные знания по языкам программирования, используемых при решении задач вычислительной математики	Демонстрирует исчерпывающие знания по языкам программирования, используемых при решении задач вычислительной математики
	У2 Уметь решать типовые задачи вычислительной математики с применением методов программирования	Не умеет решать типовые задачи вычислительной математики с применением методов программирования	Умеет решать типовые задачи вычислительной математики с применением методов программирования, допуская значительные неточности и погрешности	Умеет решать типовые задачи вычислительной математики с применением методов программирования, допуская незначительные неточности и погрешности	В совершенстве умеет решать типовые задачи вычислительной математики с применением методов программирования
	В2 Владеть навыками решения задач профессиональной деятельности с использованием современных языков программирования	Не владеет навыками решения задач профессиональной деятельности с использованием современных языков программирования	Владеет навыками решения задач профессиональной деятельности с использованием современных языков программирования, допуская значительные ошибки в расчетах	Владеет навыками решения задач профессиональной деятельности с использованием современных языков программирования, допуская незначительные ошибки в расчетах	В совершенстве владеет навыками решения задач профессиональной деятельности с использованием современных языков программирования

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

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1.	Богатырев. В. А. Информационные системы и технологии. Теория надежности : учебное пособие для бакалавриата и магистратуры / В. А. Богатырев. — Москва : Издательство Юрайт, 2019. — 318 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. https://www.biblio-online.ru/bcode/433723	ЭР	20	100	+
2.	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. https://www.biblio-online.ru/bcode/441287	ЭР	20	100	+
3.	Методы оценки и измерения характеристик информационных систем [Электронный ресурс] : Учебное пособие / И. Ю. Коцюба, А. В. Чунаев, А. Н. Шиков. - Методы оценки и измерения характеристик информационных систем, 2022-10-01. - Санкт-Петербург : Университет ИТМО,2016	ЭР*-	20	100	+
4.	Васюков, О. Г. Управление данными : учебно-методическое пособие / О. Г. Васюков. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 162 с. — ISBN 978-5-9585-0608-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/43424.htm	ЭР	20	100	±

ЭР* - электронный ресурс без ограничения числа одновременных подключений к ЭБС.

Заведующий кафедрой _____ С.К. Туренко
«3» сентября 2019 г.
Директор БИК _____ Л.Х. Каюкова
«4» сентября 2019 г.
М.П.