

Документ подписан простой электронной подписью  
Информационный сертификат:  
ФИО: Клочков Юрий Сергеевич  
Должность: и.о. ректора  
Дата подписания: 08.04.2024 14:47:40  
Уникальный программный ключ:  
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«ТОМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»**

**УТВЕРЖДАЮ**

Заместитель директора по УМР

\_\_\_\_\_ Н.В. Зонова  
« \_\_\_\_ » \_\_\_\_\_ 2022 г.

**РАБОЧАЯ ПРОГРАММА**

дисциплины:	<b>Информационная безопасность и защита информации</b>
направление подготовки:	<b>09.03.02 Информационные системы и технологии</b>
направленность (профиль):	<b>Информационные системы и технологии в геологии и нефтегазовой отрасли</b>
форма обучения:	<b>очная</b>

Рабочая программа разработана для обучающихся по направлению подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) «Информационные системы и технологии в геологии и нефтегазовой отрасли»

Рабочая программа рассмотрена  
на заседании кафедры прикладной геофизики

Заведующий кафедрой прикладной геофизики \_\_\_\_\_ С. К. Туренко

Рабочую программу разработал:  
Вяткин А.И., доцент кафедры ПГФ, 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 межсетевых экранов;
- 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 и контроля 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 инструментального 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 виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
	УК-2.2. Выбирает оптимальный способ решения задач, исходя из имеющихся ресурсов и ограничений	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-2.3. Анализирует действующее законодательство и правовые нормы, регулирующие область профессиональной деятельности	В1 методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией
ПКС-5 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-5.1 Знает технологию систем управления базами данных; угрозы и средства защиты их информационной безопасности	З2 Знать языки программирования, используемые при решении задач вычислительной математики
	ПКС-5.2 Умеет выполнять проектирование, разработку, поддержку функционирования и информационной безопасности баз данных	У2 Уметь решать типовые задачи вычислительной математики с применением методов программирования

#### 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

#### 5. Структура и содержание дисциплины

##### 5.1. Структура дисциплины

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.	0		2	3	5	УК-2.1	Задания для лабораторных работ
2	2.	Сетевые угрозы	0		2	3	5	УК-2.2	Вопросы и задания для коллоквиума, Задания для лабораторных работ
3	3.	Внедрение технологий межсетевого экрана.	3		2	3	8	УК-2.3	Вопросы и задания для коллоквиума, Задания для лабораторных работ
4	4.	Технические средства обеспечения информационной безопасности.	3		2	3	8	ПКС-5.1	Вопросы коллоквиума, Задания для лабораторных работ
5	5.	Система Предотвращения вторжений IPS.	3		2	3	8	ПКС-5.2	Вопросы коллоквиума, Задания для лабораторных работ

6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	3		2	3	8	ПКС-5.2	Вопросы коллоквиума, Задания для самостоятельной работы
7	7.	Защита от компьютерных вирусов	3		2	3	8	ПКС-5.2	Вопросы коллоквиума, Задания для самостоятельной работы, Задания для лабораторной работы
8	8.	Криптографические системы.	4		2	4	10	ПКС-5.2	Вопросы коллоквиума, Задания для самостоятельной работы, Задания для лабораторной работы
9	9.	Обеспечение безопасности локальной сети.	4		2	4	10	УК-2.3	Вопросы коллоквиума, Задания для самостоятельной работы
10	10.	Защита от потери информации и отказов программно-аппаратных средств.	5		2	4	11	УК-2.2	Вопросы коллоквиума, Задания для самостоятельной работы
11	11.	Защита информационно-программного обеспечения на уровне операционных систем.	0		2	4	6	ПКС-2.У2	Вопросы коллоквиума, Задания для самостоятельной работы
12	12.	Виртуальные частные сети VPN	0		2	5	7	ПКС-5.1	Вопросы коллоквиума, Задания для самостоятельной работы
13	13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	0		2	5	7	УК-2.2	Вопросы коллоквиума, Задания для самостоятельной работы
14	14.	Управление безопасной сетью.	0		2	5	7	УК-2.3	Вопросы коллоквиума, Задания для самостоятельной работы
15	15.	Экзамен	-		-	36	36	УК-2.1 УК-2.2 УК-2.3 ПКС-5.1 ПКС-5.2	Тестирование
Итого:			28		28	88	144		

## 5.2. Содержание дисциплины.

### 5.2.1. Содержание разделов дисциплины (дидактические единицы).

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение информационную безопасность. в	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 межсетевых экранов	Списки контроля доступа ACL. Нейтрализация атак с помощью ACL. Технологии межсетевых экранов.
4.	Технические средства обеспечения информационной безопасности.	Общие вопросы организации противодействия сетевым атакам; аппаратный контроль.
5.	Система предотвращения вторжений 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 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 резервирования 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 ОС. 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 прокси-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	3	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	3	0	0	Распределение доступа в локальных сетях с использованием ACL.	Отчет по выполнению самостоятельной работы
3	3	3	0	0	Инструменты хакера. Вредоносное ПО. Распространенные сетевые атаки.	Отчет по выполнению самостоятельной работы
4	4	3	0	0	Технологии IPS. Сигнатуры IPS (набор правил обнаружения вторжений), характеристики, сигналы и действия сигнатур.	Отчет по выполнению самостоятельной работы
5	5	3	0	0	Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем.	Отчет по выполнению самостоятельной работы
6	6	3			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	3			Стандарт шифрования данных. Криптография открытых ключей. Цифровые подписи. Инфраструктура открытых ключей.	Отчет по выполнению самостоятельной работы
8	8	4			Режимы шифрования. Особенности шифрования данных в режиме реального времени.	Отчет по выполнению самостоятельной работы
9	9	4			Топологии сетей VPN. Реализация сетей VPN.	Отчет по выполнению самостоятельной работы
10	10	4			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	4			Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС.	Отчет по выполнению самостоятельной работы
12	12	5			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	5			Защита в Internet и Intranet.	Отчет по выполнению самостоятельной работы



14	14	5			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 безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.	Отчет по выполнению самостоятельной работы
15	15	36			Экзамен	
Итого:		88	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 по текущей аттестации	Баллы
1	Работа на лабораторных занятиях	0-24
2	Коллоквиум по СРС	0-6
3	Отчет по самостоятельной работе	0-7
	<b>ИТОГО</b>	<b>0-37</b>

1	Работа на лабораторных занятиях	0-24
2	Коллоквиум по СРС	0-6
3	Отчет по самостоятельной работе	0-7
	<b>ИТОГО</b>	<b>0-37</b>
1	Работа на лабораторных занятиях	0-12
2	Коллоквиум по СРС	0-7
3	Отчет по самостоятельной работе	0-7
	<b>ИТОГО</b>	<b>0-26</b>
	<b>ВСЕГО</b>	<b>0-100</b>

## 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.riipn.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

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 учебной дисциплины	Наименование помещений для проведения учебной дисциплины, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий	Адрес (местоположение) помещений для проведения учебной дисциплины
1	2	3	4
1.	Информационная безопасность и защита информации	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, Оснащенность: Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте, проектор, проекционный экран.	625001, Тюменская область, г. Тюмень, ул. Мельникай те, д. 70
		Лабораторные занятия: Производственная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте (16 шт.).	625001, Тюменская область, г. Тюмень, ул. Мельникай те, д. 70 625001, Тюменская область, г. Тюмень, ул. Володарского, д.56

### 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.

**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 (профиль): **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

	<p>B1</p> <p>методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией</p>	<p>Не владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией</p>	<p>Частично владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией</p>	<p>В основном владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией</p>	<p>Полноценно владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией</p>
ПКС-5	<p>З2</p> <p>Знать языки программирования, используемые при решении задач вычислительной математики</p>	<p>Не знает языки программирования, используемые при решении задач вычислительной математики</p>	<p>Демонстрирует знание отдельных понятий языков программирования, используемых при решении задач вычислительной математики</p>	<p>Демонстрирует достаточные знания по языкам программирования, используемых при решении задач вычислительной математики</p>	<p>Демонстрирует исчерпывающие знания по языкам программирования, используемых при решении задач вычислительной математики</p>
	<p>У2</p> <p>Уметь решать типовые задачи вычислительной математики с применением методов программирования</p>	<p>Не умеет решать типовые задачи вычислительной математики с применением методов программирования</p>	<p>Умеет решать типовые задачи вычислительной математики с применением методов программирования, допуская значительные неточности и погрешности</p>	<p>Умеет решать типовые задачи вычислительной математики с применением методов программирования, допуская незначительные неточности и погрешности</p>	<p>В совершенстве умеет решать типовые задачи вычислительной математики с применением методов программирования</p>

## КАРТА

**обеспеченности дисциплины 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 в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Информационные системы и технологии. Теория надежности : Учебное пособие / В. А. Богатырев. - М. : Издательство Юрайт, 2018	-	20	100	+
2	Информационные системы и технологии. Теория надежности : Учебное пособие / В. А. Богатырев. - М. : Издательство Юрайт, 2018	-	20	100	+
3	Надежность и безопасность программного обеспечения : Учебное пособие / О. В. Казарин. - М. : Издательство Юрайт, 2018	-	20	100	+
4	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	+
5	Управление данными [] : учебно-методическое пособие / Васюков О. Г. - Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014	-	20	100	+