

Документ подписан простой электронной подписью
Информационный сертификат:
ФИО: Клочков Юрий Сергеевич
Должность: и.о. ректора
Дата подписания: 03.04.2024 10:20:02
Уникальный программный ключ:
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образо-
вательное учреждение высшего образования

«НОМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заведующий кафедрой
Прикладной геофизики

_____ С.К. Туренко
« ____ » _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Информационная безопасность и защита информации**

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

направленность (профиль): **Информационные системы и технологии в геологии
и нефтегазовой отрасли**

форма обучения: **очная**

Рабочая программа рассмотрена
на заседании кафедры прикладной геофизики
протокол №10 от 26.04.2023г.

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.

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 выбрать оптимальные способы их решения, исходя из действующих правовых норм, имеющих ресурсы и ограничений	УК-2.1. Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	31 виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность Уметь: У1 формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта Владеть: В1 навыком постановки задач, необходимых для достижения цели проекта
ПКС-5 Способность выполнять работы по обеспечению функционирования баз	ПКС-5.1 Знает технологию систем управления базами данных; угрозы и средства защиты их информационной безопасности	32 Знать языки программирования, используемые при решении задач вычислительной математики

данных и обеспечению их информационной безопасности	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.	2		-	3	5	УК-2.1	Задания для лабораторных работ, написание реферата
2	2.	Сетевые угрозы	2		-	3	5	УК-2.1	Задания для лабораторных работ, написание реферата
3	3.	Внедрение технологий межсетевого экрана.	2		3	3	8	УК-2.1	Задания для лабораторных работ, написание реферата
4	4.	Технические средства обеспечения информационной безопасности.	2		3	3	8	ПКС-5.1	Задания для лабораторных работ, написание реферата
5	5.	Система Предотвращения вторжений IPS.	2		3	3	8	ПКС-5.2	Задания для лабораторных работ, написание реферата
6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	2		3	3	8	ПКС-5.2	Задания для лабораторных работ, написание реферата

7	7.	Защита от компьютерных вирусов	2		3	8	ПКС-5.2	Задания для лабораторных работ, написание реферата	
8	8.	Криптографические системы.	2		4	10	ПКС-5.2	Задания для лабораторных работ, написание реферата	
9	9.	Обеспечение безопасности локальной сети.	2		4	10	УК-2.1	Задания для лабораторных работ, написание реферата	
10	10.	Защита от потери информации и отказов программно-аппаратных средств.	2		5	11	УК-2.1	Задания для лабораторных работ, написание реферата	
11	11.	Защита информационно-программного обеспечения на уровне операционных систем.	2		-	4	6	ПКС-5.2	Задания для лабораторных работ, написание реферата
12	12.	Виртуальные частные сети VPN	2		-	5	7	ПКС-5.1	Задания для лабораторных работ, написание реферата
13	13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	2		-	5	7	УК-2.1	Задания для лабораторных работ, написание реферата
14	14.	Управление безопасной сетью.	2		-	5	7	УК-2.1	Задания для лабораторных работ, написание реферата
15	15.	Экзамен	-	-	-	36	36	УК-2.1 ПКС-5.1 ПКС-5.2	вопросы к экзамену
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 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 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; аппаратуроконтроля.
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 проxy-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 межсетевых экранов.
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.	Подготовка к лабораторной работе, написание реферата

2	2	3	0	0	Распределение доступа в локальных сетях с использованием ACL.	Подготовка к лабораторной работе написание реферата
3	3	3	0	0	Инструменты хакера. Вредоносное ПО. Распространенные сетевые атаки.	Подготовка к лабораторной работе
4	4	3	0	0	Технологии IPS. Сигнатуры IPS (набор правил обнаружения вторжений), характеристики, сигналы и действия сигнатур.	Подготовка к лабораторной работе написание реферата
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.	Подготовка к лабораторной работе написание реферата
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.	Подготовка к лабораторной работе написание реферата
7	7	3			Стандарт шифрования данных. Криптография открытых ключей. Цифровые подписи. Инфраструктура открытых ключей.	Подготовка к лабораторной работе написание реферата
8	8	4			Режимы шифрования. Особенности шифрования данных в режиме реального времени.	Подготовка к лабораторной работе
9	9	4			Топологии сетей VPN. Реализация сетей VPN.	Подготовка к лабораторной работе написание реферата
10	10	4			Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога	Подготовка к лабораторной работе
11	11	4			Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС.	Подготовка к лабораторной работе
12	12	5			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
13	13	5			Защита в Internet и Intranet.	Подготовка к лабораторной работе

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.	Подготовка к лабораторной работе
Итого:		52	0	0		

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

- решение задач, выполнение практических заданий, проектов (лабораторные работы);
- работа в малых группах (лабораторные работы);
- 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
1	Выполнение лабораторных работ (1-4)	0-16
	Итого за I аттестацию	0-16
4	Выполнение лабораторных работ(5-8)	0-16
5	Защита реферата	0-21
	Итого за II аттестацию	0-37

7	Выполнение лабораторных работ(9-11)	0-12
8	Тестирование	0-35
	Итого за III аттестацию	0-47
	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:

- 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>
 - Национальная электронная библиотека (НЭБ)
 - 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>
 - Электронная справочная система нормативно-технической документации «Технорматив»
 - ЭКБСОН- информационная система доступа к электронным каталогам библиотек сферы образования и науки.
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	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 и защита информации	<p>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.</p> <p>Лабораторные занятия: Производственная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте (16 шт.).</p>	<p>625001, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70</p> <p>625001, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70</p>

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: **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. 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	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
		Уметь: У1 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 основном умеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта	Полноценно умеет формулировать взаимосвязанные задачи, обеспечивающие достижение цели проекта

		Владеть: В1 навыком постановки задач, необходимых для достижения цели проекта	Частично владеет навыком постановки задач, необходимых для достижения цели проекта	В основном владеет навыком постановки задач, необходимых для достижения цели проекта	Полноценно владеет навыком постановки задач, необходимых для достижения цели проекта
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	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
	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	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

КАРТА

обеспеченности дисциплины (модуля) учебной и учебно-методической литературойДисциплина: **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 вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2022. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490026	ЭР*	20	100	+
2	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435	ЭР*	20	100	+
3	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 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/43424.htm	ЭР*	20	100	+

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

Лист согласования

Внутренний документ "Информационная безопасность и защита информации_2023_09.03.02_ИСТНБ"

Серийный номер ЭП	Должность	ФИО	ИО	Результат	Дата	Комментарий
	Заведующий кафедрой, имеющий ученую степень доктора наук		Туренко Сергей Константинович	Согласовано		
	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		
	Директор		Каюкова Дарья Хрисановна	Согласовано		