

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: ПАНОВ Юрий Петрович
Должность: Ректор
Дата подписания: 09.06.2025 11:34:26
Уникальный программный ключ:
e30ba4f0895d1683ed43800960e77389e6cbff62

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Практикум по решению научно-исследовательских задач профессиональной деятельности
рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Промышленной кибербезопасности и защиты геоданных		
Учебный план	s100503_25_BZO25.plx	Специальность	10.05.03 Информационная безопасность автоматизированных систем
Квалификация	Специалист по защите информации		
Форма обучения	очная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах:	
в том числе:		зачеты 6	
аудиторные занятия	70,25		
самостоятельная работа	37,75		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
	14			
Неделя	14			
Вид занятий	УП	РП	УП	РП
Практические	70	70	70	70
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	70,25	70,25	70,25	70,25
Контактная работа	70,25	70,25	70,25	70,25
Сам. работа	37,75	37,75	37,75	37,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Цели: Получение практических навыков научно-исследовательской деятельности в лабораторных условиях путем непосредственного участия студентов в решении актуальных научно-технических задач с раскрытием индивидуальных особенностей и способностей. Задачи: Подготовка студентов к самостоятельной работе в сфере информационной безопасности. Применение студентами знаний и умений, полученных при изучении дисциплин специальности для решения междисциплинарных задач в сфере информационной безопасности. Овладение навыками анализа имеющихся ресурсов и управления ими для решения поставленных задач обеспечения защиты информации.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:		Б1.В.10
2.1	Требования к предварительной подготовке обучающегося:	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Кодирование информации в автоматизированных системах управления	
2.2.2	Математическое моделирование информационных потоков и систем защиты информации	
2.2.3	Автоматизированные системы управления	
2.2.4	Современные киберугрозы в промышленных и корпоративных системах автоматизации	
2.2.5	Цифровая обработка сигналов в системах обеспечения информационной безопасности автоматизированных систем управления	
2.2.6	Методы интеллектуального анализа данных в обеспечении информационной безопасности	
2.2.7	Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1: Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации

Знать:

Уровень 1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
Уровень 2	назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно-исследовательской работы; основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;
Уровень 3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучения по прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения;
Уметь:	
Уровень 1	использовать методы проведения физических исследований, технические и программные средства для

	<p>анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями;</p>
Уровень 2	<p>составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;</p>
Уровень 3	<p>формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей; анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ;</p>
Владеть:	
Уровень 1	<p>навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно-исследовательской работы; навыком составления математических моделей дискретных систем и сигналов;</p>
Уровень 2	<p>навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчетов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем;</p>
Уровень 3	<p>навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности;</p>

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.2	Уметь:
3.3	Владеть:

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность)						
1.1	Методика НИР: основные этапы /Пр/	6	6,3	ПК-1	Л1.1	4	
1.2	Поиск и формулировка проблемы ИБ, составление перечня ключевых слов. /Пр/	6	6,3	ПК-1	Л1.1	0	

1.3	Поиск научной литературы в русскоязычных электронных ресурсах /Пр/	6	6,3	ПК-1	Л1.1	0	
1.4	Поиск научной литературы в зарубежных электронных ресурсах /Пр/	6	6,3	ПК-1	Л1.1	0	
1.5	Поиск экспертной информации по проблеме /Пр/	6	6,3	ПК-1	Л1.1	0	
1.6	Поаспектная систематизация и отбор выявленной литературы /Пр/	6	6,3	ПК-1	Л1.1	0	
1.7	Поаспектное реферирование выявленной литературы /Пр/	6	6,3	ПК-1	Л1.1	0	
1.8	Аналитико-синтетическая переработка информации /Пр/	6	6,3	ПК-1	Л1.1	0	
1.9	Подготовка текста по научной проблеме ИБ /Пр/	6	6,3	ПК-1	Л1.1	0	
1.10	Оформление текста и Списка использованной литературы, подготовка Презентации. /Пр/	6	6,3	ПК-1	Л1.1	0	
1.11	Защита НИР /Пр/	6	7	ПК-1	Л1.1	0	
1.12	Поиск и аналитико-синтетическая обработка информации по проблемам ИБ /Ср/	6	37,75	ПК-1	Л1.1	0	
1.13	Зачет /ИВКР/	6	0,25	ПК-1	Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Практикум по решению научно-исследовательских задач профессиональной деятельности" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.

Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:

- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 6 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Шевченко О. А., Морозов П. Е., Кудряшова С. Н., Багусова Е. С., Свередюк М. Г.	Медицинское право: учебник для вузов	Санкт-Петербург: Лань, 2024

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	<p>Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся</p>	<p>Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точки доступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие</p>	
------	--	--	--

		<p>требованиям по обеспечению безопасности.</p> <p>Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе:</p> <p>средства защиты информации от НСД;</p> <p>программно-аппаратный комплекс доверенной нагрузки;</p> <p>антивирусные программные комплексы;</p> <p>межсетевые экраны;</p> <p>средства создания модели разграничения доступа;</p> <p>программа контроля полномочий доступа к информационным ресурсам;</p> <p>программа фиксации и контроля исходного состояния программного комплекса;</p> <p>программа поиска и гарантированного уничтожения информации на дисках;</p> <p>аппаратные средства аутентификации пользователя;</p> <p>системы обнаружения вторжений и анализа защищенности;</p> <p>средства анализа защищенности компьютерных сетей;</p> <p>сканеры безопасности;</p> <p>устройства чтения смарт-карт и радиометок;</p> <p>программно-аппаратные комплексы защиты информации;</p> <p>средства криптографической защиты информации.</p> <p>Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД.</p> <p>Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД.</p> <p>УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации.</p> <p>Аппаратно-программные комплексы в составе:</p> <p>аппаратно-программные средства управления</p>	
--	--	--	--

		<p>доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.</p>	
Ауд. 8	<p>Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8</p>	<p>Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).</p>	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Практикум по решению научно-исследовательских задач профессиональной деятельности" представлены в Приложении 2 и включают в себя:

1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.