МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова»
Министерства здравоохранения Российской Федерации
ФГАОУ ВО РНИМУ им Н.И.Пирогова Минздрава России (Пироговский Университет)

Институт клинической психологии и социальной работы

УТВЕРЖДАЮ

Директор Института

Никишина Вера Борисовна

Доктор психологических наук,
Профессор

_____

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.В.О.03 Основы информационной безопасности
для образовательной программы высшего образования - программы Специалитета
по направлению подготовки (специальности)
37.05.02 Психология служебной деятельности
направленность (профиль)
Психология безопасности

Москва 2025

Настоящая рабочая программа дисциплины Б.1.В.О.03 Основы информационной безопасности (далее – рабочая программа дисциплины) является частью программы Специалитета по направлению подготовки (специальности) 37.05.02 Психология служебной деятельности. Направленность (профиль) образовательной программы: Психология безопасности.

Форма обучения: очная

Составители:

№	Фамилия, Имя, Отчество	Учёная степень, звание	Должность	Место работы	Подпись
1	Сотников Владислав Андреевич	кандидат психологических наук	Заведующий кафедрой общей психологии и психологии развития	ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет)	
2	Чернов Дмитрий Николаевич	кандидат психологических наук, доцент	доцент	ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет)	

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры (протокол № _____ от «___» _____ 20___).

Рабочая программа дисциплины рекомендована к утверждению рецензентами:

№	Фамилия, Имя, Отчество	Учёная степень, звание	Должность	Место работы	Подпись

1	Казарян Мария Юрьевна	кандидат психологических наук	доцент	ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет)	

Рабочая программа дисциплины рассмотрена и одобрена советом института Институт клинической психологии и социальной работы (протокол № _____ от «___» _____ 20___).

Нормативно-правовые основы разработки и реализации рабочей программы дисциплины:

1. Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности 37.05.02 Психология безопасности, утвержденный приказом Министерства науки и высшего образования Российской Федерации от «31» августа 2020 г. No 1137 рук;
2. Общая характеристика образовательной программы;
3. Учебный план образовательной программы;
4. Устав и локальные акты Университета.

1. Общие положения

1.1. Цель и задачи освоения дисциплины

1.1.1. Цель.

Целью освоения дисциплины «Основы информационной безопасности» являются формирование целостной научной системы знаний о понятиях, закономерностях и методах обеспечения информационной безопасности, об основах и принципах защиты информации и противодействия угрозам безопасности информации.

1.1.2. Задачи, решаемые в ходе освоения программы дисциплины:

- Формирование системных теоретических, научных и прикладных знаний об основных задачах и принципах информационной безопасности, о методическом обеспечении защиты от информационных угроз безопасности; о нормативном регулировании вопросов информационной безопасности; о месте информационной безопасности в системе национальной безопасности Российской Федерации;
- Формирование и развитие умений и навыков анализировать жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; определять современные средства и способы обеспечения информационной безопасности; подбирать основные методики анализа угроз и рисков информационной безопасности;
- Формирование опыта практической деятельности в выявлении источников угроз безопасности информации и определении мер по предотвращению действия угрожающих факторов; обнаружении факторов, воздействующих на информацию при ее обработке в автоматизированных (информационных) системах; обоснования принципов построения защищенных информационных систем;
- Развитие профессионально важных качеств личности, значимых для реализации формируемых компетенций.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» изучается в 9 семестре (ах) и относится к части, формируемой участниками образовательного процесса, блока Б.1 дисциплины. Является обязательной дисциплиной.

Общая трудоемкость дисциплины составляет 2.0 з.е.

Для успешного освоения настоящей дисциплины обучающиеся должны освоить следующие дисциплины: Информатика и информационные технологии в профессиональной деятельности; Коммуникативное поведение в цифровой среде; Психологическое обеспечение служебной деятельности; Юридическая психология; Основы кибербезопасности; Правоведение; Криминальная психология; Психологическое консультирование; Психология влияния; Психология массовых манипуляций; Практика по профилю профессиональной деятельности.

Знания, умения и опыт практической деятельности, приобретенные при освоении настоящей дисциплины, необходимы для успешного прохождения практик: Исследовательская практика; Преддипломная практика.

1.3. Планируемые результаты освоения дисциплины

Семестр 9

Код и наименование компетенции	
Код и наименование индикатора достижения компетенции	**Планируемые результаты освоения дисциплины (модуля)**
ПК-2 Способен осуществлять мониторинг психологической безопасности и комфортности среды проживания населения	
ПК-2.ИД1 Выделяет критерии психологической безопасности людей в зависимости от социальной ситуации	**Знать:** понятия конфиденциальности, тайны и государственной тайны; критерии психологической безопасности в области информационной безопасности в зависимости от социальной ситуации; правила безопасного поведения в информационной среде
	Уметь: характеризовать понятие «психологическая безопасность» и ее взаимосвязь с информационной безопасностью; распознавать потенциальные угрозы безопасности и принимать меры для их устранения; анализировать социальные ситуации, в которых можно столкнуться с угрозами в области информационной безопасности, и вырабатывать соответствующие стратегии, направленные на защиту от этих угроз
	Владеть практическим опытом (трудовыми действиями): идентификации типичных угроз информационной безопасности, связанных с различными социальными ситуациями; применения методов и техник, позволяющих обеспечить психологическую безопасность в информационном пространстве
ПК-2.ИД2 Осуществляет мониторинг критериев психологической безопасности населения в различных социальных условиях	**Знать:** критерии, используемые для мониторинга психологической безопасности населения в области информационной безопасности; социальные условия и риски, влияющие на защищённость информации
	Уметь: использовать инструменты мониторинга для получения и анализа данных о психологической и информационной безопасности населения; выявлять риски информационной безопасности, влияющие на психологическую безопасность населения

	Владеть практическим опытом (трудовыми действиями): разработки стратегий улучшения психологической безопасности на основе мониторинга угроз информационной безопасности; создания рекомендаций по улучшению психологической безопасности населения в различных социальных условиях с учетом защищенности информации
ПК-2.ИД3 Применяет результаты мониторинга психологической безопасности и комфортности среды проживания для подбора и разработки инструментария для профилактической консультационной и психокоррекционной работы, направленной на улучшение состояния и динамики психологического здоровья населения	**Знать:** факторы информационной безопасности, влияющие на психологическое здоровье населения; классификацию типов угроз информационной безопасности населения
	Уметь: оценивать эффективность профилактических и психокоррекционных методов работы с психологической безопасностью населения с учетом возможных угроз информационной безопасности; определять необходимые параметры для мониторинга информационной, психологической безопасности и комфортности среды проживания
	Владеть практическим опытом (трудовыми действиями): анализа показателей мониторинга для оценки психологической безопасности и комфортности среды проживания, а также формирования пакета необходимых инструментов для проведения профилактической, консультационной и психокоррекционной работы, основываясь на анализе результатов мониторинга
УК-11 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	
УК-11.ИД1 Анализирует, верно интерпретирует и правильно применяет правовые нормы о противодействии коррупционному поведению	**Знать:** основные правовые нормы и нормативные акты в области регуляции вопросов информационной безопасности; этические принципы и механизмы регуляции информационной безопасности с целью предотвращения проявлений экстремизма, терроризма и коррупционного поведения
	Уметь: анализировать ситуации, связанные с проявлениями экстремизма, терроризма и коррупционного поведения в информационной безопасности, понимать причины возникновения таких ситуаций; верно интерпретировать правовые нормы и применять их в конкретных ситуациях, связанных с информационной безопасностью

	Владеть практическим опытом (трудовыми действиями): обнаружения случаев коррупционного поведения, проявлений экстремизма и терроризма в информационной безопасности, применения правовых норм и мер по предотвращению таких ситуаций; разработки обучающих материалов для персонала по предотвращению коррупции, экстремизма и терроризма в информационной безопасности
УК-11.ИД2 Осуществляет работу с законодательными и другими нормативными правовыми актами в аспекте противодействия коррупционному поведению	**Знать:** основные понятия и термины, используемые в законодательных и нормативных актах в области противодействия коррупции, проявлений экстремизма и терроризма в информационной безопасности
	Уметь: проводить анализ законодательных и нормативных актов, касающихся противодействия проявлениям экстремизма, терроризма и коррупционного поведения в области информационной безопасности; оценивать последствия нарушений законодательства в области противодействия проявлениям экстремизма, терроризма и коррупционного поведения в информационной безопасности
	Владеть практическим опытом (трудовыми действиями): оформления отчетной документации по результатам анализа рисков и угроз защиты информации, связанных с проявлениями экстремизма, терроризма и коррупционного поведения, включая работу с законодательными и нормативно-правовыми актами

2.Формы работы обучающихся, виды учебных занятий и их трудоёмкость

Формы работы обучающихся / Виды учебных занятий / Формы промежуточной аттестации		**Всего часов**	**Распределение часов по семестрам**
			9
Учебные занятия			
Контактная работа обучающихся с преподавателем в семестре (КР), в т.ч.:		30	30
Лекционное занятие (ЛЗ)		16	16
Лабораторно-практическое занятие (ЛПЗ)		12	12
Коллоквиум (К)		2	2
Самостоятельная работа обучающихся в семестре (СРО), в т.ч.:		32	32
Подготовка к учебным аудиторным занятиям		32	32
Промежуточная аттестация (КРПА), в т.ч.:		2	2
Зачет (З)		2	2
Общая трудоемкость дисциплины (ОТД)	в часах: ОТД = КР+СРО+КРПА+СРПА	64	64
	в зачетных единицах: ОТД (в часах)/32	2.00	2.00

3. Содержание дисциплины

3.1. Содержание разделов, тем дисциплины

9 семестр

№ п/п	Шифр компетенции	Наименование раздела (модуля), темы дисциплины	Содержание раздела и темы в дидактических единицах
Раздел 1. Теоретические основы информационной безопасности			
1	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 1. Введение в информационную безопасность	Понятие информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Классификация информации по видам тайны и степеням конфиденциальности
2	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 2. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Понятия государственной тайны и конфиденциальной информации. Организационная структура системы защиты информации
3	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности. Национальные интересы РФ в информационной сфере
Раздел 2. Методология и методы обеспечения безопасности и защиты информации			
1	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 1. Обзор защищаемых объектов и систем	Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Системная классификация угроз безопасности информации
2	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 2. Организационно-правовое обеспечение защиты информации	Организационно-правовое обеспечение защиты информации. Каналы и методы несанкционированного доступа к информации. Методы оценки уязвимости информации
3	УК-11.ИД1,	Тема 3. Методы нарушения	Методы нарушения конфиденциальности,

	УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	конфиденциальности, целостности и доступности информации	целостности и доступности информации. Функционирование системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности
4	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 4. Преступления в сфере информации и информационных технологий	Преступления в сфере информации и информационных технологий. Вредоносные программы и средства борьбы с ними. Основные понятия и задачи криптографии
5	УК-11.ИД1, УК-11.ИД2, ПК-2.ИД1, ПК-2.ИД2, ПК-2.ИД3	Тема 5. Программные и программно-аппаратные средства защиты информации	Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации

3.2. Перечень разделов, тем дисциплины для самостоятельного изучения обучающимися

Разделы и темы дисциплины для самостоятельного изучения обучающимися в программе не предусмотрены.

4. Тематический план дисциплины.

4.1. Тематический план контактной работы обучающихся с преподавателем.

№ п/п	Виды учебных занятий / форма промеж. аттестации	Период обучения (семестр) Порядковые номера и наименование разделов. Порядковые номера и наименование тем разделов. Темы учебных занятий.	Количество часов контактной работы	Виды контроля успеваемости	Формы контроля успеваемости и промежуточной аттестации		
					КП	ОП	ОК
1	2	3	4	5	6	7	8
9 семестр							
Раздел 1. Теоретические основы информационной безопасности							
Тема 1. Введение в информационную безопасность							
1	ЛЗ	Введение в информационную безопасность.	2	Д	1		
2	ЛПЗ	Информация, сообщения, информационные процессы как объекты информационной безопасности. Классификация информации по видам тайны и степеням конфиденциальности.	2	Т	1		1
Тема 2. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи							
1	ЛЗ	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	2	Д	1		
2	ЛПЗ	Понятия государственной тайны и конфиденциальной информации. Организационная структура системы защиты информации.	2	Т	1		1
Тема 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности							
1	ЛЗ	Международная, национальная и	2	Д	1		

		ведомственная нормативная правовая база в области информационной безопасности.					
2	К	Текущий рубежный (модульный) контроль по разделу 1.	2	Р	1	1	
Раздел 2. Методология и методы обеспечения безопасности и защиты информации							
Тема 1. Обзор защищаемых объектов и систем							
1	ЛЗ	Обзор защищаемых объектов и систем.	2	Д	1		
2	ЛПЗ	Понятие «угроза информации». Понятие «риска информационной безопасности». Системная классификация угроз безопасности информации.	2	Т	1		1
Тема 2. Организационно-правовое обеспечение защиты информации							
1	ЛЗ	Организационно-правовое обеспечение защиты информации.	2	Д	1		
2	ЛПЗ	Каналы и методы несанкционированного доступа к информации. Методы оценки уязвимости информации.	2	Т	1		1
Тема 3. Методы нарушения конфиденциальности, целостности и доступности информации							
1	ЛЗ	Методы нарушения конфиденциальности, целостности и доступности информации.	2	Д	1		
2	ЛПЗ	Функционирование системы защиты информации. Защита человека от опасной информации и от не	2	Т	1		1

		информированности в области информационной безопасности.					
Тема 4. Преступления в сфере информации и информационных технологий							
1	ЛЗ	Преступления в сфере информации и информационных технологий.	2	Д	1		
2	ЛПЗ	Вредоносные программы и средства борьбы с ними. Основные понятия и задачи криптографии.	2	Т	1		1
Тема 5. Программные и программно-аппаратные средства защиты информации							
1	ЛЗ	Программные и программно-аппаратные средства защиты информации. Работа с кадрами и внутриобъектовый режим.	2	Д	1		

Текущий контроль успеваемости обучающегося в семестре осуществляется в формах, предусмотренных тематическим планом настоящей рабочей программы дисциплины.

Формы проведения контроля успеваемости и промежуточной аттестации обучающихся /виды работы обучающихся

№ п/п	**Формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся (ФТКУ)**	**Виды работы обучающихся (ВРО)**
1	Контроль присутствия (КП)	Присутствие
2	Опрос письменный (ОП)	Выполнение задания в письменной форме
3	Опрос комбинированный (ОК)	Выполнение заданий в устной и письменной форме

4.2. Формы проведения промежуточной аттестации

9 семестр

1) Форма промежуточной аттестации - Зачет

2) Форма организации промежуточной аттестации -Контроль присутствия, Опрос комбинированный

5. Структура рейтинга по дисциплине

5.1. Критерии, показатели проведения текущего контроля успеваемости с использованием балльно-рейтинговой системы.

Рейтинг по дисциплине рассчитывается по результатам текущей успеваемости обучающегося. Тип контроля по всем формам контроля дифференцированный, выставляются оценки по шкале: "неудовлетворительно", "удовлетворительно", "хорошо", "отлично". Исходя из соотношения и количества контролей, рассчитываются рейтинговые баллы, соответствующие системе дифференцированного контроля.

9 семестр

Виды занятий		**Формы текущего контроля успеваемости /виды работы**		**Кол-во контролей**	**Макс. кол-во баллов**	**Соответствие оценок рейтинговым баллам*** **				
						ТК	**ВТК**	**Отл.**	**Хор.**	**Удовл.**
Лабораторно-практическое занятие	ЛПЗ	Опрос комбинированный	ОК	6	300	В	Т	50	34	17
Коллоквиум	К	Опрос письменный	ОП	1	700	В	Р	700	467	234
Сумма баллов за семестр					1000					

5.2. Критерии, показатели и порядок промежуточной аттестации обучающихся с использованием балльно-рейтинговой системы. Порядок перевода рейтинговой оценки обучающегося в традиционную систему оценок

Порядок промежуточной аттестации обучающегося по дисциплине (модулю) в форме зачёта

По итогам расчета рейтинга по дисциплине в 9 семестре, обучающийся может быть аттестован по дисциплине без посещения процедуры зачёта, при условии:

Оценка	**Рейтинговый балл**
Зачтено	600

6. Фонд оценочных средств по дисциплине (модулю) для проведения текущего контроля и промежуточной аттестации

9 семестр

Перечень вопросов для подготовки к промежуточной аттестации в форме зачёта

1. Понятие информации и информационной безопасности
2. Информация, сообщения, информационные процессы как объекты информационной безопасности
3. Целостность, доступность и конфиденциальность информации
4. Классификация информации по видам тайны и степеням конфиденциальности
5. Понятия государственной тайны и конфиденциальной информации
6. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Организационная структура системы защиты информации
7. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности
8. Законодательные акты в области защиты информации
9. Российские и международные стандарты, определяющие требования к защите информации
10. Национальные интересы РФ в информационной сфере
11. Приоритетные направления в области защиты информации в РФ
12. Система сертификации РФ в области защиты информации, основные правила и документы
13. Понятие «угроза информации»
14. Понятие «риска информационной безопасности»
15. Системная классификация угроз безопасности информации
16. Методы нарушения конфиденциальности, целостности и доступности информации
17. Каналы и методы несанкционированного доступа к информации
18. Методы оценки уязвимости информации
19. Преступления в сфере информации и информационных технологий
20. Функционирование системы защиты информации
21. Организационно-правовое обеспечение защиты информации
22. Защита человека от опасной информации
23. Защита человека от не информированности в области информационной безопасности
24. Вредоносные программы и средства борьбы с ними
25. Основные понятия и задачи криптографии
26. Программные и программно-аппаратные средства защиты информации
27. Инженерная защита и техническая охрана объектов информатизации

28. Организационно-распорядительная защита информации
29. Работа с кадрами и внутриобъектовый режим
30. Методы контроля доступа к информации

Зачетный билет для проведения зачёта

Федеральное государственное автономное образовательное учреждение
высшего образования «Российский национальный исследовательский медицинский университет
имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации
ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет)

Зачетный билет №____

для проведения зачета по дисциплине Б.1.В.О.03 Основы информационной безопасности
по программе Специалитета
по направлению подготовки (специальности) 37.05.02 Психология служебной деятельности
направленность (профиль) Психология безопасности

1. Понятие информации и информационной безопасности
2. Методы нарушения конфиденциальности, целостности и доступности информации

Заведующий Сотников Владислав Андреевич
Кафедра общей психологии и психологии развития ИКПСР

7. Методические указания обучающимся по освоению дисциплины

Для подготовки к занятиям лекционного типа обучающийся должен

Внимательно прочитать материал предыдущей лекции; ознакомиться с учебным материалом по учебнику, учебным пособиям, а также электронным образовательным ресурсам с темой прочитанной лекции; внести дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради; записать возможные вопросы, которые следует задать преподавателю по материалу изученной лекции.

Для подготовки к занятиям лабораторно-практического типа обучающийся должен

Внимательно изучить теоретический материал по конспекту лекции, учебникам, учебным пособиям, а также электронным образовательным ресурсам; подготовиться к выступлению на заданную тему; выполнить письменную работу; подготовить доклад, презентацию.

Для подготовки к коллоквиуму обучающийся должен

Изучить учебный материал по теме занятия или отдельным значимым учебным вопросам, по которым будет осуществляться опрос.

При подготовке к зачету необходимо

Изучить учебный материал по наиболее значимым темам и (или) разделам дисциплины в семестре.

Самостоятельная работа студентов (СРС) включает в себя

Работу с учебной, учебно-методической и научной литературой, электронными образовательными ресурсами (например, просмотр видеолекций или учебных фильмов), конспектами обучающегося: чтение, изучение, анализ, сбор и обобщение информации, её конспектирование; решение задач, выполнения письменных заданий и упражнений; подготовку слайдов, выполнение иных практических заданий; подготовку тематических сообщений и выступлений; выполнение письменных контрольных работ.

8. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

8.1. Перечень литературы по дисциплине:

№ п/п	Наименование, автор, год и место издания	Используется при изучении разделов	Количество экземпляров в библиотеке	Электронный адрес ресурсов
1	2	3	4	5
1	Информационная безопасность: учебное пособие для вузов, Суворова Г. М., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/informacionnaya-bezopasnost-531084
2	Психология безопасности: учебное пособие для вузов, Донцов А. И., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/psihologiya-bezopasnosti-509485
3	Тьюторство как форма психолого-педагогического сопровождения адаптации студентов в вузе: монография, Глотова Ж. В., Грошева Л. В., Николаичева В. Ю., 2018	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://www.iprbookshop.ru/75039.html
4	Информатика и основы компьютерных знаний: [учебное пособие для высших учебных заведений], Капустинская В. И., Стародубцева Л. В., Устинов А. Г., 2021	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	1	
5	Информационные	Методология и	0	https://www.

	технологии в социальной сфере: учебное пособие для бакалавров, Гасумова С. Е., 2015	методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности		studentlibrary.ru/book/ISBN9785394022364.html
6	Методы активного социально-психологического обучения: учебник и практикум для вузов, Штроо В. А., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/metody-aktivnogo-socialno-psihologicheskogo-obucheniya-511274
7	Компьютерные технологии обучения: учебник для вузов, Черткова Е. А., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/kompyuternye-tehnologii-obucheniya-513395
8	Психологическая служба в образовании: учебное пособие для вузов, Савинков С. Н., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/psihologicheskaya-sluzhba-v-obrazovanii-519832
9	Основы психологического консультирования: учебник, Ишкова М. А., 2020	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://www.studentlibrary.ru/book/ISBN97859765242791.html
10	Психологическое консультирование: учебник для вузов, Немов Р. С., 2023	Методология и методы обеспечения безопасности и защиты информации	0	https://urait.ru/book/psihologicheskoe-konsultirovanie-510719

		Теоретические основы информационной безопасности		
11	Здоровьесберегающие технологии в образовании: учебное пособие для вузов, Айзман Р. И., Мельникова М. М., Косованова Л. В., 2023	Методология и методы обеспечения безопасности и защиты информации Теоретические основы информационной безопасности	0	https://urait.ru/book/zdorovesberegayuschie-tehnologii-v-obrazovanii-513369

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе профессиональных баз данных, необходимых для освоения дисциплины (модуля)

1. ГАРАНТ https://www.garant.ru/
2. Консультант Плюс http://www.consultant.ru/
3. Каталог национальных стандартов https://www.gost.ru/portal/gost/home/standarts/catalognational
4. ЭБС «Консультант студента» www.studmedlib.ru
5. ЭБС «Айбукс» https://ibooks.ru/
6. ЭБС «Лань» https://e.lanbook.com/
7. ЭБС «ЮРАЙТ» https://urait.ru/
8. ЭБС «IPR BOOKS» https://www.iprbookshop.ru/
9. ЭБС «Букап» https://www.books-up.ru/
10. Полнотекстовая коллекция ведущих журналов по биомедицинским исследованиям «Pub Med» https://pubmed.ncbi.nlm.nih.gov/
11. Реферативная и аналитическая база научных публикаций и цитирования издательства Elsevier «Scopus» https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=#basic
12. База рефератов и полных текстов научных статей PNAS Online https://www.pnas.org/
13. Аналитическая и цитатная база данных журнальных статей компании Thomson Reuters «Web of Science» https://clarivate.com/
14. Российская государственная библиотека https://www.rsl.ru/
15. Российская национальная библиотека https://nlr.ru/
16. Государственная публичная научно-техническая библиотека России https://www.gpntb.ru
17. Электронная библиотечная система РНИМУ https://library.rsmu.ru/resources/e-lib/els/

8.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при наличии)

1. Автоматизированный информационный комплекс «Цифровая административно-образовательная среда РНИМУ им. Н.И. Пирогова»
2. Система управления обучением
3. Office Standard/ Professional Plus 2010 with SP1, дог. № 65164326 от 08.05.2015 (32 шт.), АО «СофтЛайн Трейд», срок действия лицензии: бессрочно
4. Mozilla Firefox, Mozilla Public License, www. Mozilla.org/MPL/2.0, (32 шт.), срок действия лицензии: бессрочно
5. Google Chrom, www.google.ru/intl/ru/chrom/browser/privacy/eula _text.html, (32 шт.), срок действия лицензии: бессрочно
6. 7-Zip, GNU Lesser General Public License, www.gnu.org/licenses/lgpl.html, (32 шт.), срок действия лицензии: бессрочно
7. FastStone Image Viewer, GNU Lesser General Public License, (32 шт.), срок действия лицензии: бессрочно
8. Windows 8.1 Enterprise Windows 8.1 Professional, дог. № 65162986 от 08.05.2015, (32 шт.), АО «СофтЛайн Трейд», срок действия лицензии: бессрочно
9. MTS Link
10. Adobe Reader, get/adobe.com/ru/reader/otherversions, (32 шт.), срок действия лицензии: бессрочно
11. Adobe Flash Player, get/adobe.com/ru/flashplayer/otherversions, (32 шт.), срок действия лицензии: бессрочно

8.4. Материально-техническое обеспечение дисциплины (модуля)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), как на территории Университета, так и вне ее.

Электронная информационно-образовательная среда университета обеспечивает:

- доступ к учебному плану, рабочей программе дисциплины, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочей программе дисциплины;

- формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

Университет располагает следующими видами помещений и оборудования для материально-технического обеспечения образовательной деятельности для реализации образовательной программы дисциплины (модуля):

№ п/п	Наименование оборудованных учебных аудиторий	Перечень специализированной мебели, технических средств обучения
1	Аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная мультимедийными и иными средствами обучения	Ноутбук, Проектор мультимедийный , Экран для проектора
2	Учебные аудитории для проведения промежуточной аттестации	Ноутбук
3	Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации	учебная мебель (столы, стулья), компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения (состав определяется в рабочей программе дисциплины и подлежит обновлению при необходимости). Библиотечный фонд укомплектован

печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочей программе дисциплины, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочей программе дисциплины и подлежит обновлению (при необходимости).

Обучающиеся из числа инвалидов обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Приложение 1
к рабочей программе
дисциплины (модуля)

Сведения об изменениях в рабочей программе дисциплины (модуля)

_____

для образовательной программы высшего образования – программы бакалавриата/специалитета /магистратуры (оставить нужное) по направлению подготовки (специальности) (оставить нужное) _____ (код и наименование направления подготовки (специальности)) направленность (профиль) «_____» на _____ учебный год.

Рабочая программа дисциплины с изменениями рассмотрена и одобрена на заседании кафедры _____ (Протокол № _____ от «___» _____ 20___).

Заведующий кафедрой _____(подпись)

_____(Инициалы и фамилия)

Приложение 2
к рабочей программе
дисциплины (модуля)

Формы проведения текущего контроля успеваемости и промежуточной аттестации

Формы проведения текущего контроля успеваемости и промежуточной аттестации	**Сокращённое наименование**	
Контроль присутствия	Присутствие	КП
Опрос письменный	Опрос письменный	ОП
Опрос комбинированный	Опрос комбинированный	ОК

Виды учебных занятий и формы промежуточной аттестации

Формы проведения текущего контроля успеваемости и промежуточной аттестации	**Сокращённое наименование**	
Лекционное занятие	Лекция	ЛЗ
Лабораторно-практическое занятие	Лабораторно-практическое	ЛПЗ
Коллоквиум	Коллоквиум	К
Зачет	Зачет	З

Виды контроля успеваемости

Формы проведения текущего контроля успеваемости и промежуточной аттестации	**Сокращённое наименование**	
Текущий дисциплинирующий контроль	Дисциплинирующий	Д
Текущий тематический контроль	Тематический	Т
Текущий рубежный контроль	Рубежный	Р
Промежуточная аттестация	Промежуточная аттестация	ПА