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.О.18 Основы кибербезопасности
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.О.18 Основы кибербезопасности (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	Изюмова Ирина Александровна	кандидат психологических наук	старший преподаватель	ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет)	
2	Сотников Владислав Андреевич	кандидат психологических наук	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	Радчикова Наталия Павловна	кандидат психологических наук, доцент	доцент	ФГБОУ ВО МПГУ	

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 кибербезопасности» является получение обучающимися системы теоретических, научных и прикладных знаний об основах обеспечения безопасности оборудования, программного обеспечения, информационных систем, информационных ресурсов и других данных от потенциальных цифровых угроз, актуальных проблемах правового регулирования рынка информационных ресурсов, правил обеспечения безопасности данных в организациях, в том числе в учреждениях служебной деятельности, в том числе при реализации научно-исследовательской деятельности и осуществлении трудовых функций в дальнейшей практической деятельности в особых условиях и при выполнении специальных задач.

1.1.2. Задачи, решаемые в ходе освоения программы дисциплины:

- Формирование и развитие умений и навыков применения правил кибербезопасности во всех сферах деятельности, в том числе в дальнейшей профессиональной деятельности, навыков безопасного поведения при работе с информационными отечественными и зарубежными базами, умения соблюдать нормы информационной этики и права;
- Формирование опыта практической деятельности в использовании средств информационных технологий в решении научно-исследовательских и организационных задач с соблюдением требований эргономики, техники безопасности, правовых и этических норм, норм информационной безопасности; в анализе информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- Развитие профессионально важных качеств личности, значимых для реализации формируемых компетенций;
- Формирование системных теоретических, научных и прикладных знаний об основах безопасности в информационном обществе, базовых понятиях в обеспечении основ кибербезопасности объектов различного уровня, связанных с информационными технологиями, нормативно-правовых актах, национальных, межгосударственных и международных стандартах в области защиты информации о процессах управления информационной безопасностью ресурсов в практической работе психолога в учреждениях служебной деятельности; основных организационных мерах по защите информации.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы кибербезопасности» изучается в 7 семестре (ах) и относится к обязательной части блока Б.1 дисциплины. Является обязательной дисциплиной.

Общая трудоемкость дисциплины составляет 3.0 з.е.

Для успешного освоения настоящей дисциплины обучающиеся должны освоить следующие дисциплины: Политология; Информатика и информационные технологии в профессиональной деятельности; Социальная психология; Коммуникативное поведение в цифровой среде; Психологическое обеспечение служебной деятельности; Психология и профилактика отклоняющегося поведения.

Знания, умения и опыт практической деятельности, приобретенные при освоении настоящей дисциплины, необходимы для успешного освоения дисциплин: Основы информационной безопасности; Психологическая безопасность образовательной среды; Психологическая безопасность системы здравоохранения; Психологическая безопасность субъекта профессиональной деятельности.

Знания, умения и опыт практической деятельности, приобретенные при освоении настоящей дисциплины, необходимы для успешного прохождения практик: Практика по профилю профессиональной деятельности.

1.3. Планируемые результаты освоения дисциплины

Семестр 7

Код и наименование компетенции	
Код и наименование индикатора достижения компетенции	**Планируемые результаты освоения дисциплины (модуля)**
ОПК-15 Способен при выполнении задач профессиональной деятельности планировать и организовывать служебную деятельность исполнителей, осуществлять контроль и учет ее результатов	
ОПК-15.ИД1 Осуществляет планирование и организацию служебной деятельности исполнителей при выполнении задач профессиональной деятельности	**Знать:** механизмы информационного воздействия; информационные методы изучения и обеспечения социально-психологических аспектов безопасности; социально-психологические характеристики информационной безопасности; нормативно-правовые средства обеспечения информационно-психологической безопасности личности и общества
	Уметь: планировать организацию служебной деятельности при выполнении задач профессиональной деятельности с использованием информационных методов изучения и с учетом обеспечения информационно-психологической безопасности
	Владеть практическим опытом (трудовыми действиями): планирования служебной деятельности исполнителей при выполнении задач профессиональной деятельности с использованием информационных методов изучения и с учетом обеспечения информационно-психологической безопасности
ОПК-15.ИД2 Осуществляет контроль и учет результатов служебной деятельности исполнителей при выполнении задач профессиональной деятельности	**Знать:** классификацию результатов информационного управления (когнитивный эффект, ценностные и критериальные ориентации, эффект действия); основные функции информационного управления (информирующая, организация поведения, коммуникационная)
	Уметь: формулировать потенциальные последствия информационного воздействия при выполнении исполнителями различных задач профессиональной деятельности в учреждениях служебной деятельности, в том числе в особых условиях

	Владеть практическим опытом (трудовыми действиями): прогнозирования потенциальных последствий информационного воздействия при выполнении исполнителями задач профессиональной деятельности в учреждениях служебной деятельности, в том числе в особых условиях
ОПК-8 Способен организовывать и осуществлять общую, специальную и целевую психологическую подготовку сотрудников, военнослужащих и (или) отдельных лиц к профессиональной деятельности	
ОПК-8.ИД3 Осуществляет общую, специальную и целевую психологическую подготовку сотрудников, военнослужащих и (или) отдельных лиц к профессиональной деятельности	**Знать:** основы работы в базовых компьютерных программах, нормативные правовые акты и ведомственнные документы, касающиеся работы с персональными данными и конфиденциальной информацией, методы математико-статической обработки данных; современные наукометрические системы
	Уметь: подбирать современные методики и технологии по общей, специальной и целевой психологической подготовки для сотрудников профессиональнослужебной деятельности, военнослужащих и (или) отдельных лиц к профессиональной деятельности с использованием безопасных информационных систем
	Владеть практическим опытом (трудовыми действиями): планирования мероприятий по оптимизации психологической подготовки для сотрудников, военнослужащих и (или) отдельных лиц к профессиональной деятельности с использованием современных информационных систем
ПК-2 Способен осуществлять мониторинг психологической безопасности и комфортности среды проживания населения	
ПК-2.ИД2 Осуществляет мониторинг критериев психологической безопасности населения в различных социальных условиях	**Знать:** организационные аспекты мониторинга психологической безопасности и комфортности среды; определение психологических критериев соответствия среды проживания населения; категориальнотерминологический аппарат информационной безопасности; виды информационно-психологического воздействия на человека
	Уметь: классифицировать и оценивать угрозы информационной безопасности, информационно-психологической безопасности личности, общества и государства

	Владеть практическим опытом (трудовыми действиями): использования источников профессиональной терминологии в области информационной безопасности и формулирования критериев информационно-психологической безопасности населения в различных социальных условиях
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	
УК-8.ИД1 Анализирует социальные и социально-психологические факторы и риски, негативно влияющие на жизнедеятельность	**Знать:** современные информационные системы; современные отечественные и зарубежные наукометрические системы; методы количественной и качественной обработки данных; классификацию и содержание факторов риска, негативно влияющих на жизнедеятельность; понятия информационного противоборства, информационной войны и формы их проявлений в современном мире
	Уметь: анализировать потенциальное влияние цифровых угроз при использовании современных информационных и наукометрических систем при поиске актуальной профессиональной информации; прогнозировать возможные риски, негативно влияющие на жизнедеятельность при возникновении цифровых угроз
	Владеть практическим опытом (трудовыми действиями): проведения анализа информационной безопасности применения современных информационных и наукометрических систем на этапах поиска актуальной профессиональной информации; опытом анализа влияния цифровых угроз и кибератак в различных сферах на возникновение потенциальных рисков, негативно влияющие на жизнедеятельность

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**
			7
Учебные занятия			
Контактная работа обучающихся с преподавателем в семестре (КР), в т.ч.:		34	34
Лекционное занятие (ЛЗ)		18	18
Лабораторно-практическое занятие (ЛПЗ)		14	14
Коллоквиум (К)		2	2
Самостоятельная работа обучающихся в семестре (СРО), в т. ч.:		60	60
Подготовка к учебным аудиторным занятиям		40	40
Иные виды самостоятельнои работы (в т.ч. выполнение практических задании проектного, творческого и др. типов)		20	20
Промежуточная аттестация (КРПА), в т.ч.:		2	2
Зачет (З)		2	2
Общая трудоемкость дисциплины (ОТД)	в часах: ОТД = КР+СРО+КРПА+СРПА	96	96
	в зачетных единицах: ОТД (в часах)/32	3.00	3.00

3. Содержание дисциплины

3.1. Содержание разделов, тем дисциплины

7 семестр

№ п/п	Шифр компетенции	Наименование раздела (модуля), темы дисциплины	Содержание раздела и темы в дидактических единицах
Раздел 1. Информационная безопасность и кибербезопасность			
1	УК-8.ИД1, ОПК-8.ИД3, ОПК-15. ИД2, ОПК-15.ИД1, ПК-2.ИД2	Тема 1. Информационная безопасность и кибербезопасность	Общая характеристика информации как объекта правового регулирования. Понятие и состав информационного правоотношения. Законодательство в области цифровой безопасности. Понятие цифровой безопасности. Правонарушения в информационной сфере и ответственность за их совершение. Телекоммуникационная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Теоретические концепции информационного общества. Информатизация и глобализация. Объекты информационной безопасности. Соотношение понятий «информационная безопасность» и «кибербезопасность». Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности. Основные этапы развития средств информационных технологий
Раздел 2. Механизмы обеспечения кибербезопасности			
1	УК-8.ИД1, ОПК-8.ИД3, ОПК-15. ИД2, ОПК-15.ИД1, ПК-2.ИД2	Тема 1. Механизмы обеспечения кибербезопасности	Основные аспекты информационной безопасности. Информация и безопасность, информационная безопасность: определение понятий. Стратегия в области информационно-коммуникационных технологий. Глобальная культура кибербезопасности и защита важнейших информационных инфраструктур.

			Использование информационно-коммуникационных технологий в целях развития. Достижения в сфере информатизации и телекоммуникаций. Преступное использование информационных технологий и меры борьбы. Национальная стратегия кибербезопасности Российской Федерации. Национальные стратегии кибербезопасности других государств. Региональные механизмы обеспечения кибербезопасности

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
7 семестр							
Раздел 1. Информационная безопасность и кибербезопасность							
Тема 1. Информационная безопасность и кибербезопасность							
1	ЛЗ	Понятие информации. Теоретические концепции информационного общества.	2	Д	1		
2	ЛПЗ	Понятие информации. Теоретические концепции информационного общества.	2	Т	1		1
3	ЛЗ	Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.	2	Д	1		
4	ЛПЗ	Объекты информационной безопасности. Соотношение понятий «информационная безопасность» и «кибербезопасность».	2	Т	1		1
5	ЛЗ	Модели, ресурсы, технологии и мишени информационных воздействий.	2	Д	1		
6	ЛЗ	Объекты информационной безопасности.	2	Д	1		
7	ЛЗ	Основы обеспечения информационно	2	Д	1		

		психологической безопасности личности.					
8	ЛПЗ	Основы обеспечения информационно психологической безопасности личности.	2	Т	1		1
9	К	Текущий рубежный (модульный) контроль по разделу 1.	2	Р	1	1	
Раздел 2. Механизмы обеспечения кибербезопасности							
Тема 1. Механизмы обеспечения кибербезопасности							
1	ЛЗ	Международный механизм обеспечения кибербезопасности.	2	Д	1		
2	ЛПЗ	Международный механизм обеспечения кибербезопасности.	2	Т	1		1
3	ЛЗ	Национальные механизмы обеспечения кибербезопасности.	2	Д	1		
4	ЛПЗ	Национальные механизмы обеспечения кибербезопасности. Ч.1.	2	Т	1		1
5	ЛЗ	Региональные механизмы обеспечения кибербезопасности.	2	Д	1		
6	ЛПЗ	Национальные механизмы обеспечения кибербезопасности. Ч. 2.	2	Т	1		1
7	ЛЗ	Основные направления обеспечения информационно-психологической безопасности личности.	2	Д	1		
8	ЛПЗ	Региональные механизмы обеспечения кибербезопасности.	2	Т	1		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

7 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.

7 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	7	301	В	Т	43	29	15
Коллоквиум	К	Опрос письменный	ОП	1	700	В	Р	700	467	234
Сумма баллов за семестр					1001					

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 7 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

7 семестр

Перечень вопросов для подготовки к промежуточной аттестации в форме зачёта

1. Информационная безопасность: понятие, виды
2. Понятие информации
3. Теоретические концепции информационного общества
4. Информатизация и глобализация
5. Объекты информационной безопасности
6. Соотношение понятий «информационная безопасность» и «кибербезопасность»
7. Понятие информационно-психологическая безопасность
8. Основные аспекты информационной безопасности
9. Информация и безопасность, информационная безопасность: определение понятий
10. Международно-правового регулирования информационных отношений с точки зрения обеспечения информационной безопасности
11. Стратегия в области информационно-коммуникационных технологий
12. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур
13. Использование информационно-коммуникационных технологий в целях развития
14. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
15. Борьба с преступным использованием информационных технологий
16. Национальная стратегия кибербезопасности Российской Федерации
17. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности
18. Роль информационной безопасности в обеспечении национальной безопасности государства
19. Интересы личности и общества в информационной сфере
20. Интересы государства в информационной сфере

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.О.18 Основы кибербезопасности
по программе Специалитета
по направлению подготовки (специальности) 37.05.02 Психология служебной деятельности
направленность (профиль) Психология безопасности

1. Информационная безопасность: понятие, виды
2. Роль информационной безопасности в обеспечении национальной безопасности государства

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; 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

Закрепление и углубление полученных знаний, умений и навыков, поиск и приобретение новых знаний, выполнение учебных заданий, подготовку к предстоящим занятиям, текущему контролю успеваемости и промежуточной аттестации.

Другое

Самостоятельная работа включает выполнение практических заданий проектного, творческого типов, таких как создание кроссвордов, майндмэпов, опросов, и пр.

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	Психология безопасности: учебное пособие для вузов, Донцов А. И., 2023	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	0	https://urait.ru/book/psihologiya-bezopasnosti-509485
2	Информационная безопасность: учебное пособие для вузов, Суворова Г. М., 2023	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	0	https://urait.ru/book/informacionnaya-bezopasnost-531084
3	Тьюторство как форма психолого-педагогического сопровождения адаптации студентов в вузе: монография, Глотова Ж. В., Грошева Л. В., Николаичева В. Ю., 2018	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	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	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	1	
5	Информационные технологии в социальной сфере: учебное пособие для бакалавров, Гасумова С. Е., 2015	Информационная безопасность и кибербезопасность Механизмы	0	https://www.studentlibrary.ru/book/ISBN9785394022364.html

		обеспечения кибербезопасности		
6	Компьютерные технологии обучения: учебник для вузов, Черткова Е. А., 2023	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	0	https://urait.ru/book/kompyuternye-tehnologii-obucheniya-513395
7	Психологическая служба в образовании: учебное пособие для вузов, Савинков С. Н., 2023	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	0	https://urait.ru/book/psihologicheskaya-sluzhba-v-obrazovanii-519832
8	Здоровьесберегающие технологии в образовании: учебное пособие для вузов, Айзман Р. И., Мельникова М. М., Косованова Л. В., 2023	Информационная безопасность и кибербезопасность Механизмы обеспечения кибербезопасности	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. Российская национальная библиотека https://nlr.ru/
2. Российская государственная библиотека https://www.rsl.ru/
3. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/
4. Научная электронная библиотека PubMed https://pubmed.ncbi.nlm.nih.gov/
5. Научная библиотека Московского государственного университета https://nbmgu.ru/
6. Проект Научной библиотеки МГУ КиберЛенинка https://cyberleninka.ru/
7. Электронная библиотечная система РНИМУ https://library.rsmu.ru/resources/e-lib/els/
8. Аналитическая и цитатная база данных журнальных статей компании Thomson Reuters «Web of Science» https://clarivate.com/
9. Реферативная и аналитическая база научных публикаций и цитирования издательства Elsevier «Scopus» https://www.scopus.com
10. ЭБС «Консультант студента» www.studmedlib.ru
11. ЭБС «ЮРАЙТ» https://urait.ru/
12. ЭБС «Лань» https://e.lanbook.com/
13. ЭБС «IPR BOOKS» https://www.iprbookshop.ru/

14. Консультант студента http://www.studentlibrary.ru
15. Консультант Плюс http://www.consultant.ru/
16. ГАРАНТ https://www.garant.ru/
17. Российское психологическое общество. Официальный сайт профессиональной корпорации психологов России https://psyrus.ru/
18. Министерство здравоохранения РФ www.minzdravsoc.ru
19. Всемирная организация здравоохранения https://www.who.int/ru

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	Компьютерная техника с возможностью подключения к сети “Интернет”, Стулья, Столы, Проектор мультимедийный, Экран для проектора
2	Учебные аудитории для проведения промежуточной аттестации	Компьютерная техника с возможностью подключения к сети “Интернет”, Стулья, Столы
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