Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»
(ИМПЭ им. А.С. Грибоедова)

Международный институт психологии и логопедии

Кафедра клинической психологии

УТВЕРЖДАЮ:
И.о. директора международного
института психологии и логопедии
_____ /О.С. Ефимова/
«19» декабря 2025 г

Рабочая программа дисциплины
КИБЕРБЕЗОПАСНОСТЬ

Укрупненная группа специальностей
37.00.00 Психологические науки

Специальность 37.05.01 Клиническая психология

Специализация
«Патопсихологическая диагностика, консультирование и психотерапия»

Квалификация
Клинический психолог

Форма обучения: очная

Москва
2025

Рабочая программа дисциплины «Кибербезопасность». Специальность- 37.05.01 Клиническая психология, специализация- Патопсихологическая диагностика, консультирование и психотерапия / Д.В. Туркин – М.: ИМПЭ им. А. С. Грибоедова – 13с.

Рабочая программа дисциплины «Кибербезопасность» по специальности 37.05.01 Клиническая психология (специализация «Патопсихологическая диагностика, консультирование и психотерапия») разработана на основании «Федерального государственного образовательного стандарта - специалитет по специальности 37.05.01 Клиническая психология», утвержденного приказом Министерства образования и науки Российской Федерации от 26 мая 2020 г. N 683; Профессионального стандарта «Психолог в социальной сфере», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «14» сентября 2023 г. № 716н; Профессионального стандарта «Психолог-консультант», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 № 537н, согласована и рекомендована к утверждению.

Разработчики:	Д.В. Туркин, старший преподаватель
Ответственный рецензент:	С. В. Котовская, доктор психологических наук, зав. кафедрой педагогики и психологии ФГБОУ ИВО «Российский государственный университет социальных технологий»

Рабочая программа рассмотрена и одобрена на заседании кафедры клинической психологии от 19.12.2025 протокол № 5.

Заведующий кафедрой _____/ Ефимова О.С., к.п.н., доцент
(подпись)

Согласовано от библиотеки _____/ О. Е. Степкина/
(подпись)

1. Аннотация к дисциплине

Рабочая программа дисциплины «Кибербезопасность» составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта - специалитет по специальности 37.05.01 Клиническая психология;
- Приказом Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- учебным планом (очной формы обучения), составленным на основе Федерального государственного образовательного стандарта - специалитет по специальности 37.05.01 Клиническая психология (специализация «Патопсихологическая диагностика, консультирование и психотерапия»).

Рабочая программа содержит обязательные для изучения темы по дисциплине «Кибербезопасность». Дисциплина дает представления о обеспечении безопасности в цифровой среде.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в Блок 1. Дисциплины: Часть, формируемая участниками образовательных отношений, Элективные дисциплины учебных планов по специальности 37.05.01 Клиническая психология, специализация «Патопсихологическая диагностика, консультирование и психотерапия».

Дисциплина изучается на 5 курсе в 9 семестре, форма контроля – зачет.

Цель изучения дисциплины – формирование компетенций у студентов гуманитарных направлений, связанных с основами обеспечения безопасности в цифровой среде; навыков выявления потенциальных угроз и применение методов защиты информации, выработать представления о значимости обеспечения безопасности личности в информационном обществе.

Задачи:

- овладение основными понятиями кибербезопасности и методами защиты данных, необходимыми для применения в профессиональной работе, для продолжения образования;
- интеллектуальное развитие студентов, формирование качеств мышления, необходимых для профессиональной деятельности;
- формирование представлений о целях и методах кибербезопасности;
- формирование представлений о кибербезопасности как неотъемлемой части функционирования вычислительных систем и сетей, понимания значимости вопросов кибербезопасности для будущей профессиональной деятельности.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

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

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы.

Процесс изучения дисциплины направлен на формирование компетенций, предусмотренных ФГОС ВО по специальности 37.05.01 Клиническая психология (специализация «Патопсихологическая диагностика, консультирование и психотерапия»), и на основе Профессионального стандарта «Психолог в социальной сфере», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «14» сентября 2023 г. № 716н; Профессионального стандарта «Психолог-консультант», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 № 537н.

Код компетенции	Результаты освоения ООП (содержание компетенций)	Индикаторы достижения компетенций	Формы образовательной деятельности, способствующие формированию и развитию компетенции
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-8.1 Применяет теоретические и практические знания и навыки для обеспечения безопасных условий жизнедеятельности в бытовой и профессиональной сферах	Контактная работа: Лекции Семинары Практические занятия Самостоятельная работа
		УК-8.2 Осуществляет оперативные действия по предотвращению чрезвычайных ситуаций и/или их последствий, в том числе при угрозе и возникновении военных конфликтов	Контактная работа: Лекции Семинары Практические занятия Самостоятельная работа

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетные единицы.

3.1 Объём дисциплины по видам учебных занятий (в часах)

Объём дисциплины	**Всего часов**
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (всего)	32

Аудиторная работа (всего):	32
в том числе:	
Лекции	16
Семинары, практические занятия	16
Лабораторные работы	
Внеаудиторная работа (всего):	
в том числе:	
Консультации	
Самостоятельная работа обучающихся (всего)	36
Вид промежуточной аттестации обучающегося (зачет)	4

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Разделы дисциплины и трудоемкость по видам учебных занятий

(в академических часах)

№ п/п	Разделы и/или темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)								Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации (по семестрам)
			ВСЕГО	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа	Консультации	Курсовая работа	
				Лекции	Лаборатор. практикум	Практическ. занятия / семинары					
1	Тема 1. Информационное общество	9	16	4		4	8				доклад, сообщение с презентацией
2	Тема 2. Защита информации	9	16	4		4	8				доклад, сообщение с презентацией
3	Тема 3. Защита от вредоносных программ	9	18	4		4	10				доклад, сообщение с презентацией
4	Тема 4. Кибербезопасност	9	18	4		4	10				доклад, сообщение

	ь в условиях цифровой трансформации										с презентацией
5	Консультации										
6	Вид промежуточной аттестации обучающихся (зачет)	9						4			перечень вопросов к зачету
	Всего:		72	16		16	36	4			Зачет

4.2. Содержание дисциплины, структурированное по разделам (темам)

№	*Название темы*	*Содержание лекционного курса*	*Содержание семинаров*
1	Тема 1. Информационное общество	Введение в информационное общество - Определение информационного общества: Понятие и основные характеристики. - Исторический контекст: Этапы развития от аграрного и индустриального общества к информационному. - Технологические перемены: Роль интернета, мобильной связи и цифровых технологий.	Обсуждение примеров успешных и неуспешных внедрений информационных технологий в различных областях (образование, здравоохранение, бизнес). - Проблемы конфиденциальности: Как защищать личные данные в цифровом мире. - Фейковые новости и дезинформация: Влияние на общественное мнение и демократию. - Обсуждение вопросов: Баланс между свободой информации и безопасностью общества.
2	Тема 2. Защита информации	Классификация информации - Разделение информации на категории в зависимости от уровня конфиденциальности. - Формирование политик доступа к информации.	Создание и внедрение плана реагирования на инциденты. - Ролевые игры на тему реагирования на утечки информации.
3	Тема 3. Защита от вредоносных программ	Угрозы безопасности - Виды угроз: внешние (кибератаки) и внутренние (неумышленная утечка данных, злоумышленное поведение сотрудников). - Методы анализа угроз (например, SWOT-анализ).	- Разработка программы обучения для повышения осведомленности о безопасности. - Роль культуры безопасности в организации.

		Методы защиты информации - Технические средства защиты: антивирусы, межсетевые экраны, шифрование. - Организационные меры: создание регламентов, прохождение обучения по безопасности.	
4	Тема 4. Кибербезопасность в условиях цифровой трансформации	- Влияние технологий, таких как облачные вычисления, IoT и Big Data на безопасность данных. - Примеры успешной интеграции цифровых технологий в бизнес-процессы. - Обзор типов кибератак (фишинг, DDoS, вредоносное ПО и т.д.). - Кейс-стадии известных атак и их последствия.	Оценка рисков в кибербезопасности: - Методы и инструменты для выявления и оценки рисков. - Практическое задание по анализу уязвимостей. Дискуссия по новейшим трендам: - Обсуждение актуальных тем, таких как искусственный интеллект в кибербезопасности, нулевой подход к безопасности (Zero Trust) и др.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся при изучении дисциплины «Кибербезопасность» предполагает работу с основной и дополнительной литературой. Результатами этой работы становятся выступления на семинарах, участие в обсуждении тем курса, подготовка докладов, выполнение разноуровневых индивидуальных заданий.

Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей обучающихся. Время и место выполнения самостоятельной работы выбираются обучающимися по своему усмотрению с учетом рекомендаций преподавателя.

Самостоятельную работу над дисциплиной следует начинать с изучения рабочей программы дисциплины «Кибербезопасность», которая содержит основные требования к знаниям, умениям и навыкам обучающихся. Обязательно следует учитывать рекомендации преподавателя, данные на занятиях и приступать к изучению отдельных тем в порядке, предусмотренном программой.

Получив представление об основном содержании темы на лекции, необходимо изучить и закрепить материал с помощью источников, указанных в разделе 6 рабочей программы. Целесообразно составить краткий конспект, отображающий содержание и связи основных понятий данной темы. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно, для того, чтобы была возможность обсудить эти вопросы на практическом занятии.

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Тема 1. Информационное общество	Баланс между свободой информации и безопасностью общества	Работа в библиотеке, включая ЭБС. Подготовка доклада.	Литература к курсу, работа с интернет - источниками	доклад, сообщение с презентацией, дискуссия
Тема 2. Защита информации	Ролевые игры на тему реагирования на утечки информации	Работа в библиотеке, включая ЭБС. Подготовка доклада.	Литература к курсу, работа с интернет - источниками	доклад, сообщение с презентацией, дискуссия
Тема 3. Защита от вредоносных программ	Роль культуры безопасности в организации.	Работа в библиотеке, включая ЭБС. Подготовка доклада.	Литература к курсу, работа с интернет - источниками	доклад, сообщение с презентацией, дискуссия
Тема 4. Кибербезопасность в условиях цифровой трансформации	Подготовка по вопросам семинара. Подготовка устных докладов. Подготовка реферата. Работа со статьями по специальной психологии и педагогике в периодических изданиях. Подготовка в опросу.	Обсуждение актуальных тем, таких как искусственный интеллект в кибербезопасности, нулевой подход к безопасности (Zero Trust) и др.	Литература к курсу, работа с интернет - источниками	доклад, сообщение с презентацией, дискуссия

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108023.html (дата обращения: 23.08.2023). — Режим доступа: для авторизир. Пользователей

2. Ванина А.Г. Персональная кибербезопасность : учебное пособие (курс лекций) / Ванина А.Г., Орёл Д.В., Аникуев С.В.. — Ставрополь : Северо-Кавказский федеральный университет, 2022. — 137 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135721.html (дата обращения: 17.12.2025). — Режим доступа: для авторизир. Пользователей

3. Крумина, К. В. Цифровая грамотность. В 2 частях. Ч.1. Основы цифровой грамотности и кибербезопасности : учебное пособие / К. В. Крумина, Н. А. Моисеева. — Омск : Омский государственный технический университет, 2023. — 100 с. — ISBN 978-5-8149-3701-8, 978-5-8149-3702-5 (ч.1). — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/140876.html (дата обращения: 27.06.2024). — Режим доступа: для авторизир. пользователей

Дополнительная литература:

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — 2-е изд. — Москва, Вологда : Инфра-Инженерия, 2025. — 692 с. — ISBN 978-5-9729-2520-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/154736.html (дата обращения: 24.09.2025). — Режим доступа: для авторизир. Пользователей

2. Краковский Ю.М. Защита информации : учебное пособие / Краковский Ю.М.. — Ростов-на-Дону : Феникс, 2016. — 349 с. — ISBN 978-5-222-26911-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/59350.html (дата обращения: 17.12.2025). — Режим доступа: для авторизир. Пользователей

7. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности обучающегося
Лекция	В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложных и интересных положениях изучаемого материала, которые должны быть приняты обучающимися во внимание. Обучающиеся должны конспектировать материал лекций, т.е. кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Материалы лекций необходимо систематически прорабатывать: проверять термины, понятия с помощью энциклопедий, словарей, справочников. Необходимо выделить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Материалы лекций являются основой для подготовки обучающихся к практическим занятиям.
Практические занятия	Практическое занятие направлено на углубление научно - теоретических знаний и овладение определенными способами работы, которое формирует практические умения обучающихся. Целью практических занятий является содействие овладению обучающимися навыками и умениями, необходимыми при решении практических задач. В процессе занятия обучающиеся по заданию преподавателя выполняют индивидуальные или групповые практические задания для овладения необходимыми профессиональными навыками. Обучающиеся должны систематически готовиться к практическим занятиям, актуализируя лекционный и семинарский материал по соответствующим темам, осуществлять поиск необходимой информации, выполнять предложенные преподавателем задания. Для успешного освоения материала дисциплины «Кибербезопасность» обучающиеся должны систематически посещать практические занятия.
Семинары	Целями семинаров являются: контроль за степенью усвоения пройденного материала, ходом выполнения обучающимися самостоятельной работы и

	рассмотрение наиболее сложных и спорных вопросов по изучаемой теме. В рамках темы каждого семинара предусмотрена подготовка обучающимися устных выступлений по вопросам изучаемой темы, которые предлагаются обучающимся заранее, с последующим их обсуждением всеми обучающимися в группе. На семинарах проводятся контрольные мероприятия. Для успешного освоения материала дисциплины «Кибербезопасность» обучающиеся должны систематически посещать семинары. В процессе подготовки к семинарам обучающимся в обязательном порядке необходимо знакомиться с обязательной литературой по соответствующим темам, а также, при подготовке докладов - с первоисточниками и публикациями по изучаемой теме в научной периодике, конспектируя их. На семинарах предполагается активное участие обучающихся в обсуждении конкретных вопросов, критический анализ представленных сообщений, дополнения к ответам. При подготовке к занятию обучающемуся необходимо ответить на вопросы, составить перечень вопросов, вызвавших затруднения или имеющих неоднозначную трактовку.
Устный опрос	Устный опрос регулярно проводится во время семинаров с целью проверки базовых знаний обучающихся по изученным темам. Обучающимся предлагается ответить на ряд вопросов, касающихся основных терминов и понятий, концепций и фактов по материалу изученных тем. Ответы должны быть достаточно полными и содержательными. К устному опросу должны быть готовы все обучающиеся. В процессе подготовки к устному опросу необходимо систематически изучать обязательную литературу по темам дисциплины, повторять изученный материал, опираясь на конспекты лекций.
Доклад, сообщение с презентацией	Доклад - это результат самостоятельной работы обучающегося, представляющий собою публичное выступление, в ходе которого автор раскрывает содержание темы, суть проблемы, которой посвящен доклад, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер. Выбор темы доклада осуществляется обучающимся не менее чем за неделю до планируемого выступления. Тематика докладов доводится до сведения обучающихся ведущим преподавателем. При выборе темы доклада важно учитывать ее актуальность, соответствие содержанию изучаемой темы дисциплины, научную разработанность, возможность обращения к необходимым источникам для изучения темы доклада, личный интерес к данной теме. Примерные этапы работы над докладом таковы: формулирование темы, подбор и изучение основных источников по теме; составление библиографии; систематизация информации; разработка плана; написание доклада; публичное выступление. При подготовке доклада необходимо использовать не только обязательную литературу, но и дополнительные источники. Доклад может сопровождаться слайд-презентацией. Выступающему, по окончании представления доклада, могут быть заданы вопросы по теме выступления.
Дискуссия	На занятиях по дисциплине «Кибербезопасность» может проводиться дискуссия. Тема дискуссии определяется заранее, чтобы обучающиеся имели возможность самостоятельно подготовиться к ней. В дискуссионной форме рассматриваются неоднозначные и не имеющие общего решения вопросы, касающиеся сферы семейных отношений. Эта форма занятий предполагает

	обязательное активное участие обучающихся в обсуждении, предоставление ими информационного материала для обсуждения, аргументированное отстаивание своей точки зрения, привлечение дополнительной информации по теме дискуссии, корректное участие в дискуссии. Проведение дискуссии позволяет оценить сформированность у обучающегося умения ставить проблему, обосновывать пути ее возможного разрешения, корректно и аргументировано отстаивать свою позицию в дискуссии.
Разноуровневые индивидуальные задания	Индивидуальные задания репродуктивного и реконструктивного уровней предлагаются с целью текущего контроля успеваемости обучающихся на семинарах/практических занятиях. Варианты разноуровневых индивидуальных заданий включают два вопроса по изученным темам дисциплины. Обучающийся должен дать письменные ответы на оба вопроса. При подготовке к выполнению заданий необходимо повторить материал изученных тем дисциплины. По итогам выполнения задания обучающийся должен представить письменный отчет.
Самостоятельная работа	Самостоятельная работа проводится с целью систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний обучающихся; формирования умений использовать учебную, научную и научно-практическую литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирования самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций. Формы и виды самостоятельной работы обучающихся: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; подготовка к различным формам текущей и промежуточной аттестации (к устному опросу, докладу, выполнению разноуровневых индивидуальных заданий, коллоквиуму, зачету с оценкой). Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов ИМПЭ им. А.С. Грибоедова: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов; компьютерные классы с возможностью работы в сети Интернет; учебную и учебно-методическую литературу. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультацию по выполнению задания, на которой разъясняет цель задания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся. Контроль самостоятельной работы обучающихся предусматривает: соотнесение содержания контроля с целями обучения; объективность контроля; валидность контроля (соответствие предъявляемых заданий тому,

	что предполагается проверить). Формы контроля самостоятельной работы: просмотр и проверка выполнения самостоятельной работы преподавателем; организация самопроверки, обсуждение результатов выполненной работы на занятии; проведение устного опроса.
Подготовка к зачету	При подготовке к зачету по «Кибербезопасность» необходимо повторить весь материал дисциплины, ориентируясь на перечень вопросов к зачету и используя конспекты лекций и рекомендуемую литературу. В ходе самостоятельной подготовки к зачету можно рекомендовать обучающимся письменно проработать материал, делая упор как на базовые понятия, так и на практическую составляющую курса. Это позволит лучше подготовиться к промежуточной аттестации. Зачет проводится по вопросам, охватывающим весь пройденный материал дисциплины или в форме итогового тестирования. Для успешной сдачи зачета по дисциплине «Кибербезопасность» обучающиеся должны принимать во внимание, что весь материал, представленный в перечне вопросов к зачету, нужно знать. Указанные в рабочей программе формируемые в результате освоения дисциплины профессиональные компетенции должны быть продемонстрированы обучающимся.

8.1. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета

8.1.1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

В Университете имеются специализированные аудитории для проведения занятий по информационным технологиям.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

Электронная информационно-образовательная среда Университета включает:

1. Официальный сайт Университета (https://www.iile.ru/)
2. Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)
3. Программы для ЭВМ. Система дистанционного обучения «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 02.07.2025 по 01.07.2026 г.) https://impe.lms.mirapolis.ru/mira/
4. Программа для ЭВМ. Виртуальная комната «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 02.07.2025 по 01.07.2026 г.) https://impe.lms.mirapolis.ru/mira/
5. Система тестирования INDIGO лицензионное соглашение (Договор от 07.11.2018 г. №Д-54792, дополнительное соглашение № Д-5479/6 о пролонгации договора до 01.06.2026г.) http://212.48.35.211:85/

8.1.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

(состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

1. Операционная система «Атлант» - Atlant Academ от 24.01.2024 г. (бессрочно)
2. Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition договор-оферта № Tr000941765 от 16.10.2025 г.

8.1.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется при необходимости, но не реже одного раз в год.

Перечень современных профессиональных баз данных и информационных справочных систем:

1. Информационно-поисковая система «Консультант Плюс» - Договор №МИ-ВИП-79717-56/2022 (бессрочно)
2. Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2024 г. №11652/24С (срок действия до 31.08.2027 г.) https://www.iprbookshop.ru/
3. Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2026 от 30.01.2026 г. (срок действия до 29.01.2027г.) https://elibrary.ru

8.1.4. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Раздел 9. Материально-техническое обеспечение образовательного процесса

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Оборудование: специализированная мебель (мебель аудиторная (столы, стулья, доска аудиторная навесная), стол преподавателя, стул преподавателя. Технические средства обучения: персональный компьютер; мультимедийное оборудование (проектор, экран).
Помещение для самостоятельной работы	Специализированная мебель (столы, стулья), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета