МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА)»

Кафедра уголовно-правовых наук

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Преступления против информационной безопасности

Б1.В.ДВ.04.01.

год набора 2026

Код и наименование направления подготовки:	40.04.01 Юриспруденция
Уровень высшего образования:	магистратура
Направленность (профиль) ОПОП ВО:	Уголовное право и уголовное судопроизводство
Форма (формы) обучения:	очная, заочная
Квалификация:	магистр

Москва – 2026

е

Программа утверждена на заседании кафедры уголовного права протокол № 8 от «13» февраля 2026 года

Автор:
Русскевич Е.А. – доктор юридических наук, доцент, профессор кафедры уголовного права Университета имени О.Е. Кутафина (МГЮА).

Рецензент:
Бессарабов В.А. – адвокат Межрегиональной коллегии адвокатов г. Москвы.

Русскевич Е.А.
Преступления против информационной безопасности: рабочая программа дисциплины (модуля) / Русскевич Е.А. — М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024.

Программа составлена в соответствии с требованиями ФГОС ВПО по направлению подготовки 40.04.01 Юриспруденция

Программа адаптирована кафедрой уголовного-правовых наук для Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА).

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

Виды профессиональной деятельности, к которым готовится обучающийся в рамках освоения дисциплины (модуля) «Преступления против информационной безопасности»:

– правоприменительная;

– правоохранительная;

– экспертно-консультационная.

Целью дисциплины (модуля) является овладение системой научных знаний и практических навыков по уголовно-правовому противодействию преступлениям против информационной безопасности.

Задачами дисциплины (модуля) «Преступления противинформационной безопасности» являются (1) получение обучающимися знаний по вопросам криминализации, квалификации и наказуемости преступлений против информационной безопасности; (2) приобретение ими навыков и умений применения полученных знаний в практическойдеятельности.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Преступления против информационной безопасности» (Б1.В.ДВ.04.01) относится к Блоку 1, к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы высшего образования, элективные дисциплины.

Для освоения дисциплины (модуля) «Преступления против информационной безопасности» обучающемуся требуется наличие базовых знаний в области теории государства и права, истории государства и права России, логики, отраслевых юридических дисциплин (уголовного права, уголовно-процессуального права, уголовно-исполнительного права, криминологии).

Дисциплина (модуль) «Преступления против информационной безопасности» является базовой для изучения таких учебных дисциплин (модулей), как «Сравнительное правоведение», «Теория предупреждения преступности», «Криминалистическое обеспечение безопасности предпринимательской деятельности». Она необходима для последующего усвоения профессионального цикла магистерской программы и выполнения магистерской диссертации.

1.3. Формируемые компетенции и индикаторы их достижения (планируемые результаты освоения дисциплины (модуля))

По итогам изучения дисциплины (модуля) «Преступления против информационной безопасности» обучающийся должен обладать следующими компетенциями в соответствии с ФГОС ВО:

Универсальные компетенции:

-

Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1);

Профессиональные компетенции:

- Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального и процессуального права (ПК-2);

- Способен давать юридические консультации и заключения в различных сферах юридической деятельности (ПК-3).

Разделы (темы) дисциплины (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))**
Понятие и классификация преступлений против информационной безопасности Преступления, посягающие на информацию ограниченного доступа Преступления, посягающие на информацию ограниченного доступа	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий ПК-2. Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы	ИУК 1.1Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними ИУК 1.3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников ИУК 1.4.Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов ИПК 2.1.Знает правовые принципы и действующие нормативные правовые акты с

Преступления в сфере цифровых технологий в зарубежных странах	материального и процессуального права ПК-3. Способен давать юридические консультации и заключения в различных сферах юридической деятельности	учетом специфики отдельных отраслей права ИПК 2.3.Устанавливает фактические обстоятельства, имеющие юридическое значение ИПК 2.4.Определяет характер правоотношения и подлежащие применению нормы материального и процессуального права ИПК 2.5.Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права ИПК 3.1 Выявляет и формулирует наличие правовой ИПК 3.3 Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных

В результате освоения учебной дисциплины (модуля) «Преступления против информационной безопасности» обучающийся должен:

знать:

– российское уголовное законодательство о преступлениях против информационной безопасности;

– актуальные проблемы защиты информации конфиденциального характера уголовно-правовыми средствами;

– современные уголовно-правовые методы противодействия социально опасной информации;

– основные направления борьбы с преступлениями против информационной безопасности в зарубежных странах.

уметь:

– правильно квалифицировать преступления против информационной безопасности;

– выявлять уголовно-правовые риски в информационной сфере;

– давать юридические заключения и консультации по вопросам уголовно-правовой охраны информации;

– разрабатывать уголовно-правовые акты в области применения цифровых технологий.

владеть:

– терминологией, связанной с уголовно-правовым противодействием

угрозам информационной безопасности;

– навыками поиска, обобщения и анализа судебной практики по делам о преступлениях против информационной безопасности.

II. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Тематические планы

Общая трудоемкость дисциплины (модуля) составляет 3 зачетные единицы, 108 часов.

2.1.1. Тематический план для очной формы обучения

№ п/п	Раздел (тема) учебной дисциплины	Семестр	Виды учебной деятельности и трудоемкость (в часах)			Образовательные технологии	Формы текущего контроля
			лекции	практ. занятия/ лабор.	СРС		
1	**Раздел I. Информация ограниченного доступа как предмет преступления.** Тема 1. Понятие и классификация преступлений против информационной безопасности	1	2		30	Лекция-дискуссия/ Проблемная лекция	
2	**Раздел I. Информация ограниченного**	1		4	32	Коллоквиум, доклад с презентацией,	Тестирование/ устный и письменный

	доступа как предмет преступления. Тема 2. Преступления, посягающие на информацию ограниченного доступа					управляемая дискуссия, кейс-стади, мозговой штурм, работав малых группах, написание эссе/реферата, составление схем	опрос/ контрольны езадания
3	**Раздел I. Информация ограниченног о доступа как предмет** преступления. Тема 3.ITпреступления	1		6/2 лабор. работа	30	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работав малых группах, написание эссе/реферата, составление схем	Тестирование /устный и письменный опрос/ контрольны езадания
	ИТОГО:	108	2	12 /2	92		Зачет

2.1.2. Тематический план для заочной формы обучения

№ п/п	Раздел (тема) учебной дисциплины	курс	Виды учебной деятельности и трудоемкость (в часах)			Образовательные технологии	Формы текущего контроля
			лекции	практ. занятия / лабор.	СРС		
1	**Раздел I. Информация**	1	2			Лекция	

	ограниченного доступа как предмет преступления. Тема 1. Понятие и виды преступлений против информационной безопасности				20	дискуссия/ Проблемная лекция	
2	**Раздел I. Информация ограниченного доступа как предмет преступления.** Тема 2. Преступления, посягающие на информацию ограниченного доступа	1		2	20	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
3	**Раздел I. Информация ограниченного доступа как предмет преступления.** Тема 3. ITпреступления	1		2	20	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания

4	**Раздел II. Социально опасная информация как предмет преступления.** Тема 4. Уголовноправовое противодействие социально опасной информации	1		2(2)	30	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
5	**Раздел II. Социально опасная информация как предмет преступления.**	1		2	27	Коллоквиум, доклад с презентацией, управляемая	Тестирование/ устный и письменный опрос/
	Тема 5. Преступления в сфере цифровых технологий в зарубежных странах					дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	контрольные задания
	Всего по ЗФО	108	2	8(2)	92		зачет Контроль - 4часа

2.2. Занятия лекционного типа

Первый семестр

Раздел I. Информация ограниченного характера как предмет преступления – 2 часа

Тема 1. Понятие и классификация преступлений против информационной безопасности – 6 часов

Вопросы (основное содержание) занятия лекционного типа:

1. Понятие и виды информационной безопасности. Угрозы информационной безопасности. Информационная безопасность как объект преступления
2. Информация: понятие, признаки, классификация. Информация как предмет преступления
3. Понятие и классификация преступлений против информационной безопасности. Преступления, посягающие на информацию ограниченного доступа

Задание для подготовки к занятию лекционного типа:

Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.

Второй семестр

Раздел II. Социально опасная информация как предмет преступления

Тема 2. Уголовно-правовое противодействие социально опасной информации

Вопросы (основное содержание) занятия лекционного типа:

1. Понятие и классификация социально опасной информации. Социально опасная информация как предмет преступления.
2. Уголовно-правовое противодействие деятельности, направленной на побуждение человека к поведению, опасному для его жизни и здоровья.
3. Уголовно-правовое противодействие информации противоправного характера.

Задание для подготовки к занятию лекционного типа:

Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.

2.3. Занятия семинарского типа

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Первый семестр

Раздел I. Информация ограниченного доступа как предмет преступления

Тема 1. Преступления, посягающие на информацию ограниченного доступа

Вопросы для подготовки к занятию семинарского типа:

1. Преступления, посягающие на государственную тайну.
2. Преступления, посягающие на информацию конфиденциального характера.

Задания для подготовки к заданию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Преступления, посягающие на информацию конфиденциального характера».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Преступления, посягающие на коммерческую и банковскую тайну», «Неправомерное использование инсайдерской информации», «Профессиональная и служебная тайна как предмет преступления».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3 казуса по теме.

Тема 2. IT-преступления

Вопросы для подготовки к занятию семинарского типа:

1. Понятие и виды IT-преступлений.
2. Киберпреступления: вопросы квалификации.
3. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Виды IT-преступлений».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Киберпреступления: международное и российское законодательство», «Определение места совершения трансграничных преступлений с использованием информационно-телекоммуникационных технологий».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3 казуса по теме.

Второй семестр

Раздел II. Социально опасная информация как предмет преступления

Тема 3. Уголовно-правовое противодействие социально опасной информации

Вопросы для подготовки к занятию семинарского типа:

1. Понятие и классификация социально опасной информации. Социально опасная информация как предмет преступления.
2. Уголовно-правовое противодействие деятельности, направленной на побуждение человека к поведению, опасному для его жизни и здоровья.
3. Уголовно-правовое противодействие информации противоправного характера.
4. Кибербуллинг и его формы (кибермоббинг, киберсталкинг, троллинг, хейтерство и др.) как угрозы информационной безопасности личности.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Социально опасная информация как предмет преступления».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Оскорбление чувств верующих: международное, европейское и российское законодательство», «Уголовная ответственность за репосты и лайки», «Травля в сети: уголовно-правовой аспект».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3 задачи по теме.

Тема 4. Преступления в сфере цифровых технологий в зарубежных странах

Вопросы для подготовки к занятию семинарского типа:

1. Преступления в сфере цифровых технологий по законодательству стран Западной Европы.
2. Преступления в сфере цифровых технологий по

законодательству США.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.

2. Подготовить доклады с презентациями (с их последующим обсуждением) по вопросам: «Уголовно-правовая охрана частной жизни в зарубежных странах», «Профессиональная тайна как предмет преступления: анализ зарубежного уголовного законодательства»; «Киберпреступления: сравнительно-правовой аспект»; «Уголовно-правовая характеристика незаконного оборота порнографической продукции по законодательству зарубежных стран», «Борьба с экстремистскими преступлениями в зарубежных странах».

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Первый курс

Раздел I. Информация ограниченного доступа как предмет преступления

Тема 1. Преступления, посягающие на информацию ограниченного доступа

Вопросы для подготовки к занятию семинарского типа:

1. Преступления, посягающие на государственную тайну.
2. Преступления, посягающие на информацию конфиденциального характера.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.

2. Составить схему по вопросу: «Преступления, посягающие на информацию конфиденциального характера».

3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Преступления, посягающие на коммерческую и банковскую тайну», «Неправомерное использование инсайдерской

информации», «Профессиональная и служебная тайна как предмет преступления».

4. Обобщить судебную практику по вопросам темы. 5. Составить 2-3 казуса по теме.

Тема 2. IT-преступления

Вопросы для подготовки к занятию семинарского типа:

1. Понятие и виды IT-преступлений.
2. Киберпреступления: вопросы квалификации.
3. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Виды IT-преступлений».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Киберпреступления: международное и российское законодательство», «Определение места совершения трансграничных преступлений с использованием информационно- телекоммуникационных технологий».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3 казуса по теме.

Раздел II. Социально опасная информация как предмет преступления

Тема 3. Уголовно-правовое противодействие социально опасной информации

Вопросы для подготовки к занятию семинарского типа:

1. Понятие и классификация социально опасной информации. Социально опасная информация как предмет преступления.
2. Уголовно-правовое противодействие деятельности, направленной на побуждение человека к поведению, опасному для его жизни и здоровья.
3. Уголовно-правовое противодействие информации противоправного характера.

4. Кибербуллинг и его формы (кибермоббинг, кибersталкинг, троллинг, хейтерство и др.) как угрозы информационной безопасности личности.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Социально опасная информация как предмет преступления».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Оскорбление чувств верующих: международное, европейское и российское законодательство», «Уголовная ответственность за репосты и лайки», «Травля в сети: уголовно-правовой аспект».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3задачи по теме.

Тема 4. Преступления в сфере цифровых технологий в зарубежных странах

Вопросы для подготовки к занятию семинарского типа:

1. Преступления в сфере цифровых технологий позаконодательству стран Западной Европы.
2. Преступления в сфере цифровых технологий по законодательству США.

Задания для подготовки к занятию семинарского типа:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Подготовить доклады с презентациями (с их последующим обсуждением) по вопросам: «Уголовно-правовая охрана частной жизни в зарубежных странах», «Профессиональная тайна как предмет преступления: анализ зарубежного уголовного законодательства»; «Киберпреступления: сравнительно-правовой аспект»; «Уголовно-правовая характеристика незаконного оборота порнографической продукции по законодательству зарубежных стран», «Борьба с экстремистскими преступлениями в зарубежных странах».

2.4. Самостоятельная работа

Виды самостоятельной работы:

1. Изучение законодательства, основной и дополнительной литературы по темам занятий лекционного и семинарского типа.
2. Подготовка к занятиям семинарского типа включает следующие типы самостоятельной работы обучающегося по любой форме обучения:

– составление в письменном виде схем по конкретным вопросам темы практического занятия;

– подготовка докладов с презентацией по конкретным вопросам темы практического занятия с их последующим обсуждением в ходе практического занятия в рамках управляемой дискуссии;

– обобщение судебной практики по вопросам темы практического занятия; – составление 2-3 казусов на основе обобщенной судебной практики с последующим их решением на занятиях семинарского типа.

Модельные задания для обучающихся всех форм обучения:

1. Изложение материала по отдельным вопросам, указанным к каждой теме практического занятия, в виде схемы с последующим ее обсуждением в ходе практического занятия с целью выявления достоинств и недостатков 2. Каждый обучающийся в течение семестра должен подготовить как минимум один доклад с презентацией во вопросам, сформулированным к темам занятий семинарского типа, и после его обсуждения в ходе практического занятия представить преподавателю грамотно оформленные тезисы доклада (56 страниц, кегль шрифта основного текста 14 пт., междустрочный интервал – полуторный) и презентацию. Тезисы доклада должны иметь необходимый научный аппарат (правильно оформленные ссылки на источники). В докладе должны быть рассмотрены дискуссионные точки зрения по сложным и актуальным вопросам выбранной темы, юридически грамотно сформулирована и обоснована точка зрения автора. При подготовке доклада необходимо использовать специальную литературу по теме (монографии, научные публикации в периодических изданиях). Докладчик должен быть готов отстаивать свою позицию в ходе обсуждения доклада.
3. Сбор, анализ и обобщение судебной практики с использованием сайта Росправосудие – https://rospravosudie.com и сайта Судебные и нормативные акты РФ – http://sudact.ru.
4. Составление казуса (задачи) на основе изученных уголовных дел в рамках обобщения судебной практики. С этой целью необходимо выбирать наиболее интересные решения судов по конкретным делам.
5.

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Модельные задания для контроля самостоятельной работы обучающихся и проведения текущей аттестации (темы докладов, вопросы для составления схем и др.) по отдельным разделам дисциплины (модуля) приводятся к каждому занятию лекционного и семинарского типа.

Промежуточная аттестация проводится в виде решения одного кейсстади.

Вопросы для подготовки к промежуточной аттестации в форме зачета:

1. Понятие и виды преступлений против информационной безопасности.
2. Преступления, посягающие на государственную тайну: вопросы квалификации.
3. Уголовно-правовая охрана неприкосновенности частной жизни.
4. Специальные технические средства, предназначенные для негласного получения информации, как предмет и орудие совершения преступления.
5. Уголовная ответственность за незаконное разглашение профессиональной тайны.
6. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну: вопросы квалификации.
7. Неправомерное использование инсайдерской информации.

Манипулирование рынком.

8. Понятие и виды IT-преступлений.
9. Киберпреступления: международно-правовое регулирование.
10. Неправомерный доступ к компьютерной информации.
11. Создание, использование и распространение вредоносных компьютерных программ.
12. Неправомерное воздействие на критическую информационную инфраструктуру РФ.
13. Мошенничество в сфере компьютерной информации.
14. Посягательства на сведения, составляющие тайну следствия и судопроизводства.

Вопросы для подготовки к промежуточной аттестации в виде

экзамена:

1. Понятие и виды преступлений против информационной безопасности.
2. Преступления, посягающие на государственную тайну: вопросы квалификации.
3. Уголовно-правовая охрана неприкосновенности частной жизни.
4. Специальные технические средства, предназначенные для негласного получения информации, как предмет и орудие совершения преступления.
5. Уголовная ответственность за незаконное разглашение профессиональной тайны.
6. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну: вопросы квалификации.
7. Неправомерное использование инсайдерской информации. Манипулирование рынком.
8. Понятие и виды IT-преступлений.
9. Киберпреступления: международно-правовое регулирование.
10. Неправомерный доступ к компьютерной информации.
11. Создание, использование и распространение вредоносных компьютерных программ.
12. Неправомерное воздействие на критическую информационную инфраструктуру РФ.
13. Мошенничество в сфере компьютерной информации.
14. Посягательства на сведения, составляющие тайну следствия и судопроизводства.
15. Преступления, сопряженные с побуждением человека к суицидальному поведению.
16. Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего.
17. Создание некоммерческой организации, посягающей на личность и права граждан.
18. Угроза убийством или причинением тяжкого вреда здоровью как действие и способ совершения преступления.
19. Посягательства на честь, достоинство и репутацию личности.
20. Уголовная ответственность за оборот информации порнографического характера.
21. Уголовная ответственность за оборот и сокрытие информации террористического характера.
22. Незаконный оборот наркотических средств и психотропных веществ, совершаемый с использованием сети Интернет.

23. Уголовная ответственность за оборот информации, связанной с возбуждением политической, идеологической, расовой, национальной, религиозной и социальной ненависти или вражды.

24. Публичные призывы к развязыванию агрессивной войны. Реабилитация нацизма.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Нормативные правовые акты и судебная практика:

1. Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве) от 23 ноября 2001 года (Будапешт)
2. Конвенция об обеспечении международной информационной безопасности (концепция, проект) от 22 сентября 2011 года
3. Соглашение между Правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года
4. Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности от 10 октября 2010 года
5. Модельный информационный кодекс для государств-участников СНГ. Часть первая от 3 апреля 2008 года
6. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)
7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 07.06.2017)
8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в ред. от 01.07.2017)
9. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ
10. Трудовой кодекс Российской Федерации от 30 декабря 2001 № 197-ФЗ (ред. от 03.08.2018)
11. Закон РФ от 21 июля 1993 г. № 5485-1 (в ред. от 08.03.2015) «О государственной тайне»
12. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»
13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
14. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

15. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
16. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»
17. Федеральный закон от 2 декабря 1990 г. № 395-ФЗ № 395-1-ФЗ «О банках и банковской деятельности» (с изм. и доп.)
18. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
19. Перечень сведений, отнесенных к государственной тайне (утв. Указом Президента РФ от 30 ноября 1995 г. № 1203 в ред. от 1.01.2018 № 5)
20. Указ Президента РФ от 06 марта 1997 г. № 188 (в ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»
21. Положение о Межведомственной комиссии по защите государственной тайны (утв. Указ Президента РФ от 6 октября 2004 г. № 1286)
22. Указ Президента РФ от 24 июля 2013 г. № Пр-1753 «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»
23. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»
24. Указ Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
25. Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации»
26. Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»
27. Указ Президента РФ от 09.11.2022 N 809 (ред. от 04.03.2026) "Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей"
28. Распоряжение Президента РФ от 15.01.2010 № 24-рп (ред. от 14.01.2011) «Об утверждении перечня должностей, при замещении которых лица считаются допущенными к государственной тайне»
29. Распоряжение Президента РФ от 16.04.2005 № 151-рп (ред. от 22.12.2017) «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне»
30. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности (утв. постановлением Правительства

РФ от 4 сентября 1995 г. № 870)

31. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне (утв. Постановлением Правительства РФ от 6 февраля 2010 г. № 63)
32. Положение о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне (утв. Постановлением Правительства РФ от 22 августа 1998 г. № 1003)
33. Уголовный кодекс Дании / Научное редактирование и предисловие С.С. Беляева. Перевод с датского и английского С.С. Беляева, А.Н. Рычевой. – СПб.: Изд-во «Юридический центр Пресс», 2001. – 230 с.;
34. Уголовный кодекс Испании / Пер. с фр. В.П. Зыряновой; под ред. Н.Ф. Кузнецовой, Ф.М. Решетникова. – М.: Зерцало, 1998. – 218 с.;
35. Уголовный Кодекс Франции / Науч. ред. Л.В. Головко, Н.Е. Крыловой; пер. с фр. и пред. Н.Е. Крыловой. – СПб.: Юридический Центр Пресс, 2002. – 650 с.; 35. Уголовный Кодекс ФРГ / Науч. ред., вст. ст. Д.А. Шестакова; пред. Г.-Г. Йешека; пер. с нем. Н.С. Рачковой. – СПб.: Юридический Центр Пресс, 2003. – 522 с.;
36. Уголовный кодекс Швейцарии / Науч. ред., предисловие и перевод с немец. А.В. Серебренниковой. – СПб.: Изд-во «Юридический цент Пресс», 2002. – 350 с.;
37. Уголовный кодекс Швеции / Науч. ред. Н.Ф. Кузнецовой и С.С. Беляева. Перевод С.С. Беляева. – СПб.: Изд-во «Юридический центр Пресс», 2001. – 320 с.;
38. Примерный уголовный кодекс (США). Официальный проект Института американского права / Пер. с англ. А.С. Никифорова; Под ред. и с предисл. Б.С. Никифорова. М.: Издательство «Прогресс», 1969. – 304 с.
39. Постановление Конституционного Суда РФ от 14 мая 2003 № 8-П «По делу о проверке конституционности пункта 2 статьи 14 Федерального закона «О судебных приставах» в связи с запросом Лангепасского городского суда Ханты-Мансийского автономного округа»
40. Постановление Конституционного Суда РФ от 07 июня 2012 № 14-П «По делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» и статьи 24 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина А.Н. Ильченко»
41. Определение Конституционного Суда РФ от 28 июня 2012 № 1253-

О «Об отказе в принятии к рассмотрению жалобы гражданина

Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса РоссийскойФедерации»

42. Определение Конституционного Суда РФ от 15 января 2015 № 25-О «Об отказе в принятии к рассмотрению жалобы гражданинаПушкина Сергея Александровича на нарушение его конституционных прав абзацем четвертым части первой статьи 22 Закона Российской Федерации «О государственной тайне»

43. Постановление Конституционного Суда РФ от 06 ноября 2014 № 27-П «По делу о проверке конституционности статьи 21 и статьи 21^1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина О.А. Лаптева»

44. Определение Конституционного Суда РФ от 09 июня 2015 № 1275-О «Об отказе в принятии к рассмотрению жалобы гражданина Зубкова Владимира Николаевича на нарушение его конституционных прав частями 2, 3 и 4 статьи 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»

45. Постановление Конституционного Суда РФ от 16 июня 2015 № 15-П «По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона «Об актах гражданского состояния» в связи с жалобой граждан Г.Ф. Грубич и Т.Г. Гущиной»

46. Постановление Конституционного Суда РФ от 17 декабря 2015 № 33-П «По делу о проверке конституционности пункта 7 части второй статьи 29, части четвертой статьи 165 и части первой статьи 182 Уголовнопроцессуального кодекса Российской Федерации в связи с жалобой граждан А.В. Баляна, М.С. Дзюбы и других»

47. Постановление Конституционного Суда РФ от 23 ноября 2017 № 32-П «По делу о проверке конституционности статей 21 и 21^1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина Е.Ю. Горовенко»

48. Постановление Пленума Верховного Суда РФ от 17 марта 2004 № 2 (ред. от 24.11.2015) «О применении судами Российской Федерации Трудового кодекса Российской Федерации»

49. Постановление Пленума Верховного Суда РФ от 24 февраля 2005

№ 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц»

50. Обзор практики рассмотрения судами Российской Федерации дел о защите чести, достоинства и деловой репутации, а также

неприкосновенности частной жизни публичных лиц в областиполитики, искусства, спорта от 27 мая 2016

51. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоениии растрате»

Основная литература:

1. Корабельников С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва Издательство Юрайт, 2021. — 111 с. — URL: https://urait.ru/bcode/476798

2. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. — М.: ИНФРА-М, 2023. – 351 с. – URL: https://znanium.com/catalog/document?id=415589

3. Юрченко И. А. Преступления против информационной безопасности: учебное пособие. — Москва: Проспект, 2021. — 208 с. - URL: http://ebs.prospekt.org/book/44295

Дополнительная литература:

1. Информационные технологии в юридической деятельности (правовая информатика в цифровую эпоху) = INFORMATION TECHNOLOGIES IN LEGAL PRACTICE (legal informatics in the digital age) : учебное пособие : в 2 частях / В.А. Вайпан, И.А. Ильюшин, В.А. Северин [и др.] ; под общ. ред. В.А. Вайпана ; Моск. гос. университет имени М.В.Ломоносова; Юридический фак-т; Кафедра правовой информатики, информ. технологий и цифрового права. - Москва : Юстицинформ, 2024-2025. - Текст : электронный. https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=82945&idb=0

2. Информационные технологии в юридической деятельности : учебник и практикум для среднего профессионального образования / Т.М. Беляева, А.Т. Кудинов, Н.В.Пальянова [и др.] ; под ред. С.Г. Чубукова. - 4-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2025. - 338 с. - (Профессиональное образование). - Библиогр. в конце тем. - Библиогр. в подстр. примеч. - Гриф УМО СПО. - ISBN 978-5-534-18966-7. - Текст : непосредственный. https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=8

3467&idb=0
3. Правовое регулирование квантовых коммуникаций в условиях экономики данных : сборник статей / под ред. А.В. Минбалеева ; Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА) ; Программа "Приоритет 2030". - Саратов : Амирит, 2024. - 188 с. - Библиогр. в подстр. примеч. - ISBN 978-5-00207-712-0. - Текст : непосредственный.
https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=84306&idb=0

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

5.1. Общесистемные требования к реализации ОПОП ВО

Институт располагает на праве собственности и на основании договоров материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы магистратуры по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

Обучающимся обеспечивается доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам. Полнотекстовая рабочая программа дисциплины (модуля) размещена в Цифровой научно-образовательной и социальной сети Университета (далее - ЦНОСС), в системе которой функционируют «Электронные личные кабинеты обучающегося и научно-педагогического работника». Доступ к материалам возможен через введение индивидуального пароля. ЦНОСС предназначена для создания личностно-ориентированной информационно-коммуникационной среды, обеспечивающей информационное взаимодействие всех участников образовательного процесса Университета, в том числе предоставление им общедоступной и персонализированной справочной, научной, образовательной, социальной информации посредством сервисов, функционирующих на основе прикладных информационных систем Университета.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде (далее – ЭИОС) Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории Университета, так и вне ее. Помимо электронных библиотек Университета, он обеспечен индивидуальным неограниченным доступом ко всем удаленным электронно-библиотечным системам, базам данных и справочно-правовым системам, подключенным в Университете на основании лицензионных договоров, и имеющие адаптированные версии сайтов для обучающихся с ограниченными

возможностями здоровья.

Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность одновременного доступа 100 процентов обучающихся из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее.

Электронная информационно-образовательная среда Университета обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

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

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы магистратуры;

- проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных технологий образовательного процесса;

- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет».

Фонд электронных ресурсов Библиотеки включает следующие информационные справочные системы, профессиональные базы данных и электронные библиотечные системы, состав которых определен в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости):

5.1.1. Справочно-правовые системы:

1.	Континент	сторонняя	http://continent-online.com	ООО «Агентство правовой интеграции «КОНТИНЕНТ», договоры: - № 22021712 от 09.03.2022 г. с 20.03 2022г. по 19.03.2023 г.; - № 23020811 от 06.03.2023 г. с 20.03.2023 г. по 19.03.2024 г.; - № 240020711 от 14.03.2024 г. с 20.03.2024 г. по 19.03.2025 г.; - № 25021313 от 11.03.2025 с 20.03.2025 г. по 19.03.2026 г.; - № 26021711 от 20.03.2026 г. с 20.03.2026 г. по 19.03.2027 г.

2.	Westlaw Academics	сторонняя	https://uk.westlaw.com	Филиал Акционерного общества «Томсон Рейтер (Маркетс) Юроп СА», договоры: - № ЭР-5/2022 от 27.10.2021 г., период доступа с 01.01.2022 г. по 31.12.2022 г.; - № 32211783551 от 16.11.2022 г. с 01.01.2023 г. по 31.12.2023 г.; - № ЭР-4/2023 от 30.11.2023 г. с 01.01.2024 г. по 31.12.2024 г.; - № ЭР-3/2025 от 29.10.2024 с 01.01.2025 по 31.12.2025; - № ЭР-7/2026 от 24.11.2025 с 01.01.2026 г. по 31.12.2026 г.
3.	Jus Mundi Academic Research	сторонняя	https://jusmundi.com	ООО «ИВИС», договоры: - № ЭР-4/2025 от 21.04.2025, период доступа с 23.04.2025 г. по 22.04.2026 г.; - № ЭР-1/2026 от 09.04.2026 г. с 23.04.2026 г. по 22.04.2027 г.
4.	КонсультантПлюс	сторонняя	http://www.consultant.ru	Открытая лицензия для образовательных организаций
5.	Гарант	сторонняя	https://www.garant.ru	Открытая лицензия для образовательных организаций
6.	Системы Casebook и Caselook	сторонняя	https://casebook.ru/ https://caselook.ru/	АО «ПравоТех», лицензионное соглашение №1А/2025 от 29.08.2025 г. с 01.09.2025 г. по 31.08.2026 г.

5.1.2. Профессиональные базы данных:

1.	Национальная электронная библиотека (НЭБ)	сторонняя	https://rusneb.ru	ФГБУ «Российская государственная библиотека», договор № 101/НЭБ/4615 от 01.08.2018 г. с 01.08.2018 по 31.07.2023г. (безвозмездный)
2.	Президентская библиотека имени Б.Н.	сторонняя	https://www.prlib.ru	ФГБУ «Президентская библиотека имени Б. Н. Ельцина:

	Ельцина			- Соглашение о сотрудничестве № 23 от 24.12.2010 г., бессрочно; - Дополнительное соглашение № 1 от 22.11.2024 г. (в связи с изменением типа МГЮА)
3.	НЭБ eLIBRARY.RU	сторонняя	http://elibrary.ru	ООО «РУНЕБ», договоры: - № ЭР-3/2022 от 04.03.2022 г. с 09.03.2022 г. по 09.03.2023 г.; - № SU-1494/2023 от 22.03.2023 г. с 27.03.2023 г. по 26.03.2024 г.; - № SU-1494/2024 от 28.03.2024 г. с 03.04.2024 г. по 02.04.2025 г.; - № ЭР-1/2025 от 21.03.2025 г. с 03.04.2025 г. по 02.04.2026 г.; - № SU-1494/2026 от 11.03.2026 г. с 03.04.2026 г. по 02.04.2027 г.
4.	ЛитРес: Библиотека	сторонняя	http://biblio.litres.ru	ООО «ЛитРес», договоры: - № ЭР-6/2022 от 18.03.2022 г. с 18.03.2022 г. по 17.03.2023 г.; - № 130223/Б-1-136 от 02.03.2023 г. с 18.03.2023 г. по 17.03.2024 г.; - № 210224/ИТ-Б-181 от 05.03.2024 г. с 18.03.2024 г. по 17.03.2025 г.; - № 180225/ИТ-Б-178 от 24.02.2025 г. с 18.03.2025 г. по 17.03.2026 г.; - № 240226/ИТ-Б-161 от 16.03.2026 г. с 18.03.2026 г. по 17.03.2027 г.

5.1.3. Электронно-библиотечные системы:

1.	ZNANIUM.COM	сторонняя	http://znanium.com	ООО «Научно-издательский центр ЗНАНИУМ», договоры: - № 3/2021 эбс от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № 1/2022эбс от 01.10.2021 г. с 01.01.2022 г. по

				31.12.2022 г.; - № 32211747575эбс от 07.10.2022 г. с 01.01.2023 г. по 31.12.2023 г.; - № ЭР-3/2023 от 30.11.2023 г. с 01.01.2024 г. по 31.12.2024 г.; № ЭР-2/2025 от 23.10.2024 с 01.01.2025 г. по 31.12.2025 г.; - 32515306855 от 17.10.2025 с 01.01.2026 г. по 31.12.2026 г.
2.	Book.ru	сторонняя	http://book.ru	ООО «КноРус медиа», договоры: - № ЭР-4/2022 от 01.10.2021 г. с 01.01.2022 г. по 31.12.2022 г.; - № 32211783653 от 21.10.2022 г. с 01.01.2023 г. по 31.12.2023 г.; - № ЭР-2/2023 от 30.11.2023 г. с 01.01.2024 г. по 31.12.2024 г.; - № ЭР-1/2025 от 14.10.2024 с 01.01.2025 г. по 31.12.2025 г.; - № 32515306784 от 21.10.2025 с 01.01.2026 г. по 31.12.2026 г.
3.	ВЧЗ РГБ (Виртуальный читальный зал Российской государственной библиотеки)	сторонняя	https://search.rsl.ru/	ФГБУ «Российская государственная библиотека», договоры: - № 32312116538 от 14.02.2023 г. с 02.03.2023 г. по

				01.03.2024 г.; - № 095/04/0025 от 26.02.2024 г. с 02.03.2024 г. по 01.03.2025 г.; - № 095/04/0019 от 24.02.2025 г. с 02.03.2025 г. по 01.03.2026 г.; - № 073/04/0021 от 27.02.2026 г. с 02.03.2026 г. по 01.03.2027 г.
4.	Образовательная платформа Юрайт	сторонняя	http://www.biblio-online.ru	ООО «Электронное издательство Юрайт», договоры: - № ЭР-7/2022 от 09.03.2022 г. с 03.04.2022 по 02.04.2023 г.; - № 32312233331 от 29.03.2023 г. с 03.04.2023 г. по 02.04.2024 г.; - № ЭР-1/2024 от 25.03.2024 г. с 03.04.2024 г. по 02.04.2025 г.; - № ЭР-2/2025 от 21.03.2025 с 03.04.2025 г. по 02.04.2026 г.; - № 7823 от 26.03.2026 г. с 03.04.2026 г. по 02.04.2027 г.
5.	Юстицинформ	сторонняя	https://elknigi.ru/	ООО «Юридический дом «Юстицинформ», договоры: - № ЭР-1/2023 от 30.03.2023 г. с 05.04.2023 г. по 04.04.2024 г.; - № ЭР-2/2024 от 29.03.2024 г. с 15.04.2024 г. по

				14.04.2025 г.; - № ЭР-3/2025 от 09.04.2025 с 15.04.2025 г. по 14.04.2026 г.; - № ЭР-2/2026 от 10.04.2026 г. с 15.04.2026 г. по 14.04.2027 г.
6.	Проспект	сторонняя	http://ebs.prospekt.org	ООО «Проспект», договоры: - № ЭР-3/2021 от 21.06.2021 с 03.07.2021 г. по 02.07.2022 г.; - № 32211498857 от 24.06.2022 г. с 03.07.2022 г. по 02.07.2023 г.; - № 32312506505 от 27.06.2023 с 03.07.2023 г. по 02.07.2024 г.; - № ЭР-3/2024 от 13.06.2024 с 04.07.2024 г. по 03.07.2025 г.; - № ЭР-5/2025 от 24.06.2025 с 04.07.2025 г. по 03.07.2026 г.

Университет имени О.Е. Кутафина (МГЮА) обеспечен необходимым комплектом лицензионного программного обеспечения, состав которого подлежит ежегодному обновлению.

5.2. Перечень программного обеспечения (ПО), установленного на компьютерах, задействованных в образовательном процессе по ОПОП ВО

Все аудитории, задействованные в образовательном процессе по реализации учебной дисциплины (модуля), оснащены следующим ПО:

№ №	Описание ПО	Наименование ПО, программная среда,	Вид лицензирования

		СУБД	
ПО, устанавливаемое на рабочую станцию			
1.	Операционная система	Microsoft Windows 7 Microsoft Windows 8.1 Microsoft Windows 10	Лицензия
		ООО «+АЛЬЯНС» услуги по предоставлению неисключительных прав(лицензий) на программное обеспечение. По договорам № 242-223/20 от 19.06.2020 г.	
2.	Антивирусная защита	Kaspersky Endpoint Security для Windows	Лицензия
		ООО «Програмос-Проекты» По договорам: №УТ0032987 01.07.2021 №50-223/22 от 14.07.2022 №54-223/23 от 10.08.2023 №УТ-0038516 от 16.08.2024 №735-223/25 от 02.09.2025 (на 2 года)	
3.	Офисные пакеты	Microsoft Office 2019	Лицензия
4.	Программа для ЭВМ «Виртуальный осмотр места происшествия: Учебно-методический комплекс»	По договору: 328-У от 19.02.2021 г.	Лицензия
5.	Архиваторы	WinRar	Открытая лицензия
6.	Интернет браузер	Yandex	Открытая лицензия
7.	Программа для просмотра файлов PDF	PDF24	Открытая лицензия
		Foxit Reader	Открытая лицензия
8.	Программа для просмотра файлов DJVU	DjVuviewer	Открытая лицензия
9.	Пакет кодеков	K-LiteCodecPack	Открытая лицензия
10.	Программа для редактирования фото	Picasa	Открытая лицензия
11.	Программа для работы с графикой	PaintNet	Открытая лицензия
12.	Видеоплеер	WindowsMediaPlayer	В комплекте с ОС
13.	Программа для удаленного доступа	AnyDesk	Открытая лицензия
14.	Программа для проведения конференций	Zoom	Открытая лицензия
12.	Справочно- правовые системы (СПС)	Консультант плюс	Открытая лицензия
		Гарант	Открытая лицензия
13	Услуги по поставке обновленной версии ПО ("АС Нагрузка", Планы Мини","Планы СПО")		Лицензия
		ООО "Лаборатория Математического моделирования и информационных систем" По договорам: №9113 от 16.02.2022 №1005-23 от 03.03.2023 №2480-24 от 21.03.2024 №3833-25 от 27.03.2025 №4998-26 от 30.03.2026	

5.3. Помещения для самостоятельной работы обучающихся

Помещения для самостоятельной работы обучающихся располагаются по адресу: Оренбург, ул. Комсомольская, 50. Они оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС Университета и включают в себя:

1. Электронный читальный зал:

кресло для индивидуальной работы – 3 шт.,

компьютер в сборе: системный блок корпус черный Standart-ATX накопитель SATAIII, жесткий диск 1 ТБ, мышь USB, клавиатура USB, монитор LG 21"LED – 8 шт. (компьютерная техника подключена к сети «Интернет» и обеспечивает доступ в электронную информационно-образовательную среду).

2. Аудитория для самостоятельной работы (№ 518) на 12 посадочных мест:

стол преподавателя – 1 шт.,

стул преподавателя – 1 шт.,

парты ученические – 15 шт.,

стул ученический – 15 шт.,

доска магнитная – 1 шт.,

стационарный информационно-демонстрационный стенд – 1 шт.,

компьютер в сборе: системный блок корпус черный Standart-ATX накопитель SATAIII, жесткий диск 1 ТБ, мышь USB, клавиатура USB, монитор LG 21"LED – 8 шт. (компьютерная техника подключена к сети «Интернет» и обеспечивает доступ в электронную информационно-образовательную среду).

5.4. Сведения о доступе к информационным системам и информационно-телекоммуникационным сетям, к которым обеспечивается доступ обучающихся, в том числе приспособленных для использования инвалидами и лицами с ограниченными возможностями здоровья.

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

Для инвалидов и лиц с ограниченными возможностями здоровья созданы условия доступа к информационным системам, информационно-телекоммуникационным сетям и электронным образовательным ресурсам: читальный зал располагается на первом этаже недалеко от входа, предназначенного для маломобильных групп обучающихся, рабочие места в читальном зале оборудованы современными эргономичными моноблоками с качественными экранами, а также аудио гарнитурами, на каждом компьютере имеется возможность увеличения фрагментов изображения или текста с помощью экранной лупы, озвучивания отображаемого на экране текста. В ЭБС применяются специальные адаптивные технологии для лиц с

ограниченными возможностями зрения: версия сайта для слабовидящих, эксклюзивный адаптивный лидер, программа не визуального доступа к информации, коллекция аудио изданий.

Для формирования условий библиотечного обслуживания инвалидов и лиц с ограниченными возможностями здоровья в Университете выполняется комплекс организационных и технических мероприятий:

Наличие рабочих мест в Электронном читальном зале с увеличенным пространством для работы, выделено и обозначено табличкой со знаком доступности для всех категорий инвалидности.

Обеспечено комплексное обслуживание в читальных залах:

- поиск изданий по электронному каталогу;
- возможность получения изданий из любого отдела Библиотеки.

Обеспечено удаленное обслуживание:

- официальный сайт Университета имени О.Е. Кутафина (МГЮА) – www.msal.ru и, следовательно, страничка Библиотеки, адаптирована для слабовидящих;
- возможен поиск изданий по электронному каталогу;
- возможен онлайн-заказ изданий.

Рабочее место оборудовано:

- «накладного» типа наушниками к компьютерам (у дежурного библиотекаря);
- выведена экранная лупа Windows 7 на «рабочий стол» экрана компьютера;
- бесплатной программой NVDA - NVDA программа экранного доступа для операционных систем семейства Windows, позволяющая незрячим и слабовидящим пользователям работать на компьютере выводя всю необходимую информацию с помощью речи;
- лупа ручная для чтения 90mmx13.5mm – предназначена для чтения текстов, написанных мелким шрифтом (у дежурного библиотекаря);
- линза Френеля в виниловой рамке 300*190 – удобна для просмотра страниц формата А4(у дежурного библиотекаря).