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)

КИБЕРНЕТИЧЕСКАЯ ПРЕСТУПНОСТЬ

Б1.В.ДВ.04.02

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

Подписано цифровой подписью: Великий Дмитрий Петрович
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Федеральное казначейство, CN=Федеральное казначейство
Причина: Я подтвердил целостность этого документа
Дата: 25 Июнь 2026 г. 9:25:17

Москва – 2026

Программа утверждена на заседании кафедры криминологии и уголовно-исполнительного права, протокол № 14 от 30 мая 2026 года.

Автор: Мацкевич И.М. – д.ю.н., профессор кафедры криминологии и уголовно-исполнительного права Университета имени О.Е. Кутафина (МГЮА).

Рецензент: Атагимова Э.И. – к.ю.н., старший научный сотрудник отдела научно-исследовательской работы и образовательной деятельности ФБУ НЦПИ при Минюсте России.

Мацкевич И.М. Кибернетическая преступность: рабочая программа дисциплины (модуля) / И.М. Мацкевич. – М. Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2026.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 40.04.01 Юриспруденция
Программа адаптирована кафедрой уголовного-правовых наук для Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

Целями освоения дисциплины «Кибернетическая преступность» являются:

1) получения системного знания о предупреждении и профилактики финансовой преступности;

2) формирования навыков по обеспечению личной безопасности граждан и предпринимателей в области финансовой деятельности;

3) правильная организация безопасного предпринимательства и личного поведения, связанного с финансовыми тратами, включая взаимодействие в соответствии с действующим законодательством с банками и другими государственными и общественными институтами;

4) формирование навыков по обеспечению системы безопасного поведения людей в области финансов, защиты от финансового мошенничества и других экономических преступлений;

5) воспитание нетерпимого отношения к совершению правонарушений (преступлений), посягающих на безопасность в области финансовой деятельности.

Задачи дисциплины «Кибернетическая преступность» состоят в следующем:

- качественной подготовке конкурентоспособных и компетентных профессиональных юристов, обладающих высоким уровнем правовой культуры и правосознания, знаниями в области правоохранительной и правоприменительной деятельности;

- приобретении умения применения полученных знаний в правоприменительной, правоохранительной, экспертно-консультационной, организационно-управленческой и научно-исследовательской деятельности.

Основными видами деятельности, к которым осуществляется подготовка в рамках дисциплины, являются:

а) правоприменительная:

- обоснование и принятие в пределах должностных обязанностей решений, а также совершение действий, связанных с реализацией правовых норм;

- составление юридических документов;

б) правоохранительная:

- обеспечение законности, правопорядка, безопасности личности, общества и государства;

- защита частной, государственной, муниципальной и иныхформ собственности;

- предупреждение, пресечение, выявление финансовых преступлений;

- защита прав и законных интересов юридических лиц и от-

дельных граждан;

в) экспертно-консультационная деятельность:

- оказание юридической помощи, консультирование по вопросам права;

г) организационно-управленческая деятельность:

- осуществление организационно-управленческих функций;

д) научно-исследовательская:

- участие в проведении научных исследований в соответствии с профилем своей профессиональной деятельности.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Кибернетическая преступность» (Б1.В.ДВ.04.02) относится к Блоку 1, к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы высшего образования, элективные дисциплины.

Приступая к изучению дисциплины, обучающийся должен обладать теоретическими знаниями в области теории права, гражданского права, уголовного права, финансового права, административного права, трудового права, гражданского процессуального права, арбитражно-процессуального права, уголовного процессуального права, криминалистики, криминологии и психологии.

При изучении учебной дисциплины обучающийся, в частности, должен обладать следующими входными знаниями и умениями:

в области знаний: объяснить понятие кибернетической преступности и составляющие его признаки, рассмотреть особенности теневой экономики; обозначить критерии классификаций причин и условий; дать основы профилактики правонарушений и преступлений, связанных с использованием компьютеров и цифровой деятельностью; изучить виды компьютерных преступлений; определить мошенничества с использованием компьютеров и другие преступления, связанные с цифровой деятельностью;

в области понимания: раскрыть суть цифровой экономики и деятельности, связанной с использованием компьютеров; раскрыть сутьтеневой экономики; объяснить специфику определения причин и условий компьютерных преступлений; дифференцировать возможности использования юридических знаний для предупреждения компьютерных преступлений;

в области умения, навыка: осуществлять информационно-поисковую, аналитическую деятельность по обеспечения безопасности предпринимательской деятельности и деятельности, связанной с использованием компьютеров; самостоятельно принимать решения о виктимологической профилактике; толковать и правильно применять правовые нормы в области цифровых технологий; предупреждать компьютерные преступления, выявлять и устранять причины и условия, способствующие их совершению; владеть навыками: поиска, анализа и обобщения получаемой

информации, самостоятельной научной работы, разрешения казусов и конфликтных ситуаций.

Дисциплина «Кибернетическая преступность» является необходимым элементом подготовки будущего магистра, способствует более глубокому усвоению остальных дисциплин магистерской программы, а также организации процесса написания магистерской диссертации.

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

По итогам изучения дисциплины (модуля) «Кибернетическая преступность» 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);
- Способен управлять проектом на всех этапах его жизненного цикла (УК-2).

Профессиональные компетенции:

- Способен разрабатывать нормативные правовые и локальные правовые акты в конкретных сферах юридической деятельности (ПК-1);
- Способен планировать и организовывать научные исследования, участвовать в научно-исследовательских работах по проблемам права; способен разрабатывать собственный научный проект (ПК-5).

Разделы (темы) дисциплины (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))**
Общая характеристика кибернетической преступности Понятие и виды кибернетической преступности Личность кибернетическо	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	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 разны источников ИУК 1.4.Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных

йго преступника Причины кибернетическо й преступности Кибернетическа я преступность в зарубежных странах Предупрежде ние кибернетическо й преступности	УК-2 Способен управлять проектом на всех этапах его жизненного цикла ПК-1 Способен разрабатывать нормативные правовые и локальные правовые акты в конкретных сферах юридической деятельности (ПК-5) Способен планировать и организовывать научные исследования, участвовать в научно-исследовательских работах по проблемам права; способен разрабатывать собственный научный проект	подходов ИУК 2.1. Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления ИУК 2.2.Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения ИПК ИПК 1.2.Применяет основные приемы законодательной техники при подготовке нормативных правовых актов в сфере своей профессиональной деятельности ИПК 5.1.Показывает способность проводить анализ и обобщение результатов научно-исследовательских работ с использованием современных достижений научного знания, передового отечественного и зарубежного опыта

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Тематические планы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

2.1.1. ТЕМАТИЧЕСКИЙ ПЛАН (для очной формы обучения)

№ п/	Раздел (тема) учебной	Семест	Виды учебной деятельности и трудоемкость (в часах)	Образовательные технологии	Формы текущего контроля

п	дисциплины		Лекции	Практ. занятия/ Лаборат.	СРС		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	3	2		13	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эс-се, рефе- рат, колло-квиум
2	Понятие и виды кибернетической преступности	3		2(2)	13	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эс-се, рефе- рат, колло-квиум
3	Личность кибер-преступника	3		2	13	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум

4	Причины кибернетической преступности	3		2	13	работа в малых группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
5	Криминологическая характеристика хакерских атак	3		2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах			2	13	работа в малых группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
7	Предупреждение кибернетической преступности			2	14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	ВСЕГО		**2**	**12(2)**	**92**		зачет

Дисциплина «Кибернетическая преступность» изучается в течение одного семестра. Итоговая аттестация осуществляется в форме зачета.

2.1.2. Тематический план для заочной формы обучения

№ п/п	Раздел (тема) учебной дисциплины	Семестр	Виды учебной деятельности и трудоемкость (в часах)			Образовательные технологии	Формы текущего контроля
			Лекции	Практ. занятия/ Лаборат.	СРС		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	3	2		13	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эссе, реферат, коллоквиум
2	Понятие и виды кибернетической преступности	3			13	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	3		-	13	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум

4	Причины кибернетической преступности	3		2	13	**Лаборат. занятие.** работа в малых группах, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
5	Криминологическая характеристика хакерских атак	3		2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах			2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
7	Предупреждение кибернетической преступности			2	14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	Зачет 4 ч.						
	ВСЕГО		**2**	**8(2)**	**92**		

Учебная дисциплина «Кибернетическая преступность» изучается в течение одного семестра. Итоговая аттестация осуществляется в форме зачета.

Содержание дисциплины (программа курса)

(для всех форм обучения)

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	Особенности кибернетической преступности. Взаимосвязь с экономической преступностью. Уголовно-правовая характеристика компьютерных преступлений. Структура и характер кибернетической преступности. Виды латентной кибернетической преступности. Сущность и содержание криминологической безопасности цифровой деятельности. Криминологическая безопасность поведения граждан, связанных с использованием компьютеров и цифровых технологий. Значение криминологии в ее обеспечении. Взаимосвязь криминологии в обеспечении компьютерной безопасности с науками уголовно-правового цикла, с науками гражданско-правового цикла, с науками государственно-правового цикла: задачи и особенности.
2	Понятие и виды кибернетической преступности	История кибернетической преступности. Теневая экономика и теневая деятельность, связанная с использованием цифровых технологий. Понятие, признаки и виды кибернетической преступности. Тенденции кибернетической преступности. Предупреждение корпоративных конфликтов и роль в них компьютеров и цифровой технологии. Электронные деньги и другие современные компьютерные средства: их роль в совершении преступлений.
3	Личность кибер-преступника	Понятие и структура личности кибер-преступника. Классификация и типология различных групп и типов кибер-преступников. Механизм преступного поведения личности кибер-преступника. Виды виктимологического поведения предпринимателей и значение его изучения. Компьютерная виктимность гражданина: понятие и характерные черты. Предупреждение виктимологического поведения руководителя предприятия и работников предприятия. Правовое обеспечение защиты предпринимателей и обычных граждан от компьютерных преступлений: криминологическая характеристика.

4	Причины кибернетической преступности	Детерминация кибернетической преступности. Классификация причин и условий кибернетической преступности. Социальная обусловленность кибернетической преступности. Влияние личностных факторов на кибернетическую преступность. Криминологическая характери-
		стика основных нормативных правовых актов, регламентирующих использование компьютеров и другую цифровую деятельность. Особенности работы современных коммуникационных систем: криминологическая характеристика.
5	Криминологическая характеристика хакерских атак	Криминологическая характеристика хакерской деятельности и других видов компьютерных преступлений. Взаимосвязь компьютерных преступлений с должностной преступностью и коррупцией. Криминологическая характеристика коррупции. Взаимосвязь хакерской деятельности с организованной преступностью. Криминологическая характеристика компьютерной организованной преступности. Взаимосвязь компьютерных мошенничеств с незаконной предпринимательской деятельностью. Криминологическая характеристика незаконной предпринимательской деятельности.
6	Кибернетическая преступность в зарубежных странах	Общая характеристика кибернетической преступности развитых стран. Общая характеристика кибернетической преступности стран с переходной экономикой. Общая характеристика кибернетической преступности в других странах. Структура кибернетической преступности за рубежом. Борьба с кибернетической преступностью за рубежом. Соотношение кибернетической и организованной преступности за рубежом. Электронные деньги и компьютерные мошенничества в России и за рубежом: сравнительный анализ.
7	Предупреждение кибернетической преступности	Теория предупреждения кибернетической преступности: понятие, признаки и виды. Специальные субъекты предупреждения кибернетической преступности. Методика проведения статистических исследований деятельности, связанной с цифровой экономикой. Методы проведения социологических опросов среди пользователей компьютерными сетями. Криминология интернета. Проведение анонимных опросов и анализ их результатов. Интервью, как средство предупреждения деликтов, правонарушений и преступлений. Граждане, склонные к неоправданному рискованному финансовому поведению: криминологический анализ.

2.2. Занятия лекционного типа (для очной и заочной форм обучения)

Наименование лекции	**Объ-ем часов**	**Тематика лекции**	**Задания для подготовки к лекции**
Общая характеристика кибернетической преступности ивзаимосвязь с экономической	2	Сущность и содержание криминологической безопасности цифровой деятельности. Криминологическая безопасность поведения граждан, связанных с использованием компьютеров и цифровых технолгий.	изучить и проанализировать: - нормативные акты в части правовой регламентации банковской
преступностью		Значение криминологии в ее обеспечении. Взаимосвязь криминологии в обеспечении компьютерной безопасности с науками уголовно-правового цикла, с науками гражданско-правового цикла, с науками государственно-правового цикла: задачи и особенности. Значение криминологических основ безопасности компьютерной деятельности в работе современного предпринимателя и обычного гражданина. .	деятельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой деятельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой деятельно- сти.

2.3. Занятия семинарского типа для очной (14 часов) и заочной (10 часов) форм обучения

Наименование темы	**Содержание практического занятия**

Понятие и виды кибернетической преступности	История кибернетической преступности. Теневая экономика и теневая деятельность, связанная с использованием цифровых технологий. Понятие, признаки и виды кибернетической преступности. Тенденции кибернетической преступности. Предупреждение корпоративных конфликтов и роль в них компьютеров и цифровой технологии. Электронные деньги и другие современные компьютерные средства: их роль в совершении преступлений. *Задание для подготовки:* повторить основные положения криминологической теории, найти и изучить основные действующие криминологические нормативные правовые акты, направленные против кибернетической преступности и дать их классификацию, разобраться с тем, что понимается под теневой экономикой и как легализуются незаконно полученные деньги, посредством компьютерных технологий; изучить методы и способы отмывания денег и совершения компьютерных мошенничеств
Личность кибер-преступника	Понятие и структура личности кибер-преступника. Классификация и типология различных групп и типов кибер- преступников. Механизм преступного поведения личности кибер-преступника. Виды виктимологического поведения предпринимателей и значение его изучения
	Компьютерная виктимность гражданина: понятие и характерные черты. Предупреждение виктимологического поведения руководителя предприятия и работников предприятия. Правовое обеспечение защиты предпринимателей и обычных граждан от компьютерных преступлений: криминологическая характеристика. *Задание для подготовки:* повторить криминологическую теорию личности преступника, дать криминологическую характеристику личности кибер-преступника и построить его криминологических портрет, изучить нормативные правовые акты, касающиеся защиты свидетелей и потерпевших от кибернетических преступлений.

Причины кибернетической преступности	Детерминация кибернетической преступности. Классификация причин и условий кибернетической преступности. Социальная обусловленность кибернетической преступности. Влияние личностных факторов на кибернетическую преступность. Криминологическая характеристика основных нормативных правовых актов, регламентирующих использование компьютеров и другую цифровую деятельность. Особенности работы современных коммуникационных систем: криминологическая характеристика. *Задание для подготовки:* повторить теорию причинности в криминологии, изучить основные положения нормативных правовых актов, регламентирующих безопасную цифровую деятельность, а также специфику работы правоохранительных органов в этой области, определить нормативные правовые документы, направленные на выявление причин и условий противоправного поведения, связанного с незаконным использованием компьютеров.
Криминологическая характеристика хакерских атак	Криминологическая характеристика хакерской деятельности и других видов компьютерных преступлений. Взаимосвязь компьютерных преступлений с должностной преступностью и коррупцией. Криминологическая характеристика коррупции. Взаимосвязь хакерской деятельности с организованной преступностью. Криминологическая характеристика компьютерной организованной преступности. Взаимосвязь компьютерных мошенничеств с незаконной предпринимательской деятельностью. Криминологическая характеристика незаконной предпринимательской деятельности. *Задание для подготовки:* изучить нормативные правовые акты, касающиеся деятельности, связанной с использованием компьютеров и иной цифровой деятельности; определить место должностной преступности в структуре кибернетической преступности; дать понятие незаконной предпринимательской деятельности; установить взаимосвязь кибернетической преступности с организованной преступностью.
Кибернетическая преступность в зарубежных странах	Общая характеристика кибернетической преступности развитых стран. Общая характеристика кибернетической преступности стран с переходной экономикой. Общая характеристика кибернетической преступности в других странах

	Структура кибернетической преступности за рубежом. Борьба с кибернетической преступностью за рубежом. Соотношение кибернетической и организованной преступности за рубежом. Электронные деньги и компьютерные мошенничества в России и за рубежом: сравнительный анализ. *Задание для подготовки:* изучить нормативные правовые документы, определяющие критерии отнесения одних стран к развитым, а другие страны к странам, с переходной экономикой; изучить и сравнить статистику состояния кибернетической преступности в зарубежных странах; изучить взаимосвязь финансовых преступников и руководителей организованной преступности за рубежом.
Предупреждение кибернетической преступности	Теория предупреждения кибернетической преступности: понятие, признаки и виды. Специальные субъекты предупреждения кибернетической преступности. Методика проведения статистических исследований деятельности, связанной с цифровой экономикой. Методы проведения социологических опросов среди пользователей компьютерными сетями. Криминология интернета. Проведение анонимных опросов и анализ их результатов. Интервью, как средство предупреждения деликтов, правонарушений и преступлений. Граждане, склонные к неоправданному рискованному финансовому поведению: криминологический анализ. *Задание для подготовки:* повторить основы анализа правовой статистики, методику проведения опросов, анкетирования и интервьюирования, изучить методы составления криминологических портретов личности кибер- преступников. Изучить методы проведения интервью, как средства предупреждения правонарушений, связанных с использованием компьютеров и коммуникационных систем. Определить профилактическое значение деятельности специальных подразделений в правоохранительных органах.

2.4. Самостоятельная работа студента

При изучении учебной дисциплины «Кибернетическая преступность» используются следующие виды самостоятельной работы студентов:коллоквиумы, составление анкет, списка вопросов для опросов, документов по предупреждению деликтов, правонарушений, преступлений, криминологических аналитических справок и др. Приведенный минимум может быть расширен за счет использования заданий, дополнительно разработанных в установленном порядке. Указанные виды самостоятельной работы студентов применяются при всех формах обучения.

Примерная тематика заданий:

А) Раскрыть следующие вопросы:

1. Рыночная экономика и преступность: неизбежность и последствия.
2. Теневая экономика и ее влияние на кибернетическую преступность.
3. История кибернетической преступности.
4. Возможности криминологии в обеспечении кибернетической безопасности предпринимательской деятельности.
5. Возможности криминологии в обеспечении кибернетической безопасности обычного человека.
6. Криминологическая характеристика личности кибер-преступников.
7. Криминологическая характеристика личности потерпевших от кибернетических преступлений.
8. Коррупция в компьютерных офисах.
9. Предприниматели и хакеры: точки не соприкосновения.
10. Защита от компьютерных мошенничеств: криминологический отечественный и международный опыт.

Б) Составление процессуальных и иных документов:

1. Вопросы для анкетирования руководителей предприятия, в связи с выявленными компьютерными мошенничествами на предприятии.
2. План опроса потенциальных потерпевших граждан от компьютерных преступлений.
3. Составление аналитической справки по состоянию кибернетической преступности в Москве (ином регионе по указанию преподавателя).
4. Акт о предостережении совершения компьютерных преступлений (по ситуации, предложенной преподавателем).

В) Темы эссе (для заочной формы обучения):

1. Криминология цифрой деятельности.
2. Место криминологического обеспечения кибернетической деятельности в системе наук.
3. Роль юриста в обеспечении безопасности компьютерной деятельности на предприятии, в организации и учреждении.
4. Правовая и моральная статистика: статистические методы выявления компьютерных правонарушений и преступлений.
5. Криминологическая безопасность кадровой политики в области компьютерной деятельность.
6. Компьютерное финансовое мошенничество: криминологические способы выявления и методы противодействия.
7. Криминологическая характеристика кибернетических преступлений: методы противодействия.
8. Взаимосвязь компьютерной преступности и коррупции: непотизм, фаворитизм, а также ее новые элементы.
9. Взаимосвязь кибернетической преступности с организованной преступностью.
10. Теория предупреждения кибернетической преступности.

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В разделе приводятся примерные: а) вопросы для самоконтроля, б) темы рефератов, в) модельные задания. Указанный минимум может быть дополнен за счет использования оценочных средств, разрабатываемых кафедрой в установленном порядке, а также электронных тестовых заданий, имеющихся в централизованной базе данных Университета имени О.Е. Кутафина (МГЮА) в программе http//elearn.msal.ru.

Примерные вопросы для самоконтроля:

1. История кибернетической преступности.
2. Теневая экономика и кибернетическая преступность.
3. Понятие, признаки и виды кибернетической преступности.
4. Тенденции кибернетической преступности.
5. Закономерности кибернетической преступности.
6.Структура и характер кибернетической преступности.
7.Виды латентной кибернетической преступности.
8. Детерминация кибернетической преступности.
9. Классификация причин и условий кибернетической преступности.
10. Социальная обусловленность кибернетической преступности.
11. Влияние личностных факторов на кибернетическую преступность.
12. Понятие и структура личности кибер-преступника.
13. Классификация и типология различных групп и типов компьютерных преступников.
14. Механизм преступного поведения личности кибер-преступника.
15. Виктимологические проблемы кибернетической преступности.
16. Виктимология цифровой экономики.
17.Криминологическая характеристика должностной кибернетической преступности.
18.Причины и условия должностной кибернетической преступности.
19.Криминологическая характеристика взаимосвязи коррупции и кибернетической преступности.
20.Общая характеристика кибернетической преступности за рубежом.
21.Общая характеристика кибернетической преступности в других странах.
22.Соотношение кибернетической и организованной преступности.
23.Взаимосвязь экономических преступников и кибер-преступников.
24. Понятие, признаки и виды предупреждения кибернетической преступности.
25. Специальные субъекты предупреждения кибернетической преступности.
26. Криминология Интернета.

Темы рефератов:

1. Криминологическая характеристика безопасности деятельности, связанной с коммуникационными системами.
2. Криминологическая характеристика виктимологии кибернетической деятельности.
3. Компьтерные мошенничества на предприятии: способы и методы противодействия.
4. Взаимодействие в вопросах профилактики кибернетической преступности предпринимателей и представителей правоохранительных органов.
5. Современное понятие и состояние коррупции, связанной с коммуникационными системами и меры по противодействию ей.
6. Криминологическая характеристика судебной практики по рассмотрению дел, связанных с кибернетической преступностью.
7. Криминология интернета.
8. Криминология специальных субъектов по борьбе с кибернетическими преступлениями.
9. Криминологическая характеристика компьютерного мошенничества.
10. Специальные субъекты противодействия компьютерной преступности.

Модельные задания:

1. С учетом полученных криминологических знаний разработать максимально защищенную структуру офиса предприятия.
2. Дать криминологическую характеристику законодательства, связанного с компьютерной и другой цифровой деятельностью и уязвимого с криминологической точки зрения,
3. Разработать модель виктимологического безопасного поведения пользователя компьютерами.
4. Составить договор на интернет-обслуживание с гражданином, выделив в нем криминологически значимые элементы.
5. Разработать и представить справку о состоянии кибрнетической преступности за последний год.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Нормативно-правовые акты и судебная практика:

1. Конституция Российской Федерации // Российская газета; № 237,25.12.93

2. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ // Российская газета, N 137, 27.07.2002

3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N

51-ФЗ // Российская газета, N 238-239, 08.12.1994

4. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 N 138-ФЗ // Российская газета, N 220, 20.11.2002

5. Уголовный кодекс Российской Федерации от 13.06.96 № 63- ФЗ // Собрание законодательства РФ; 17.06.96, № 25, ст. 2954

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ // Российская газета, N 256, 31.12.2001

7. Трудовой кодекс Российской Федерации от 30.12.2001 N 197- ФЗ // Российская газета , N 256, 31.12.2001

8. Федеральный закон от 12.08.95 N 144-ФЗ "Об оперативно-розыскной деятельности"// Собрание законодательства РФ; 14.08.95, № 33, ст. 3349

9. Федеральный закон от 28.01.2011 № 3-ФЗ «О полиции» // Собрание законодательства РФ; 14.02.2011, № 7, ст. 900.

10. Федеральный закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» от 11.03.92

№ 2487-1 // Российская газета, N 100, 30.04.1992.

11. Федеральный закон Российской Федерации от 26.12.95 №208-ФЗ

«Об акционерных обществах» // Российская газета , N 248, 29.12.1995

12. Федеральный закон Российской Федерации от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью» // Российская газета, N 30, 17.02.1998

13. Федеральный закон Российской Федерации "Об электронной цифровой подписи" от 10.01.2002 N 1-ФЗ // Российская газета, N 6, 12.01.2002

14. Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ

«Об информации, информационных технологиях и защите информации» // Российская газета, N 165, 29.07.2006

15. Закон Российской Федерации от 05.03.92 № 2446-1 «О безопасности» // Российская газета, N 103, 06.05.1992

16. Федеральный закон от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ; 27.06.2016, № 26 (Часть I), ст. 3851.

17. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных // Собрание законодательства РФ.2006. № 31 (часть I). Ст. 3451.

18. Федеральный закон от 07.05.2013 № 99-ФЗ «О внесении изменений в отдельные законодательные акты в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите

физических лиц при автоматизированной обработке персональных данных» // Собрание законодательства РФ. 2013. № 19. Ст. 2326.

19. Федеральный закон от 23.12.2008 № 294-ФЗ О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля // Собрание законодательства РФ, 29.12.2008, N 52 (ч. 1), ст. 629.

20.Федеральный закон от 7.05.2013 № 78-ФЗ Об уполномоченных по защите прав предпринимателей в Российской Федерации // Собрание законодательства

РФ, 13.05.2013 N 19, ст. 2305.

21.Федеральный закон от 17.01.1992 № 2202-1О прокуратуре Российской Федерации // Ведомости СНД РФ и ВС РФ", 20.02.1992, N 8, ст. 366.

22.Федеральный закон от 28.12.201 № 403-ФЗ О Следственном комитете Российской Федерации // Собрание законодательства РФ, 03.01.2011, N 1, ст. 15.

23.Указ Президента РФ от 09.05.2017 № 203 О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

24. 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"

25. Постановление Правительства РФ от 14.09.2016 N 924 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры дорожного хозяйства, требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств автомобильного и городского наземного электрического транспорта, и внесении изменений в Положение о лицензировании перевозок пассажиров автомобильным транспортом, оборудованным для перевозок более 8 человек (за исключением случая, если указанная деятельность осуществляется по заказам либо для собственных нужд юридического лица или индивидуального предпринимателя)» // Собрание законодательства РФ", 26.09.2016, N 39, ст. 5648.

26. Инструкция ЦБ РФ «Об открытии и закрытии банковских счетов по вкладам (депозитам)» от 14.09.06 № 28-И // Вестник Банка России, N 57, 25.10.2006.

27.Постановление Пленума ВАС РФ от 04.04.2014 N 23 "О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе" // URL: http://www.arbitr.ru (дата обращения 10.06.2014).

28.Пленум Верховного Суда РФ от 15 ноября 2016 № 48 О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпри- нимательской и иной экономической деятельности// Бюллетень Верховного Суда РФ, N 1, январь, 2017.

29.Методические рекомендации по осуществлению прокурорскогонадзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // http://genproc.gov.ru

Основная литература:

1. Решетников, А. Ю. Криминология [Электронный ресурс] : учебное пособие для вузов / А. Ю. Решетников, О. Р. Афанасьева. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2021. — 166 с. URL: www.biblio-online.ru/book/724EB42B-90FF-4B70-818C-EDB2BED388F5

2. Репецкая А.Л. Женская преступность: региональная криминологическая характеристика и предупреждение : монография / А.Л. Репецкая, Т.С. Кононыхина. - Москва : Юрлитинформ, 2025. - 128 с. URL: https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=81313&idb=0

3. Дашиева А.Д. Деятельность прокуратуры по предупреждению преступности и иных правонарушений : учебное пособие / А.Д. Дашиева, И.Л. Зиновьев, А.А. Кузакова ; под ред. Т.И. Отческой ; Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА). - Москва : Проспект, 2025. - 184 с. URL: https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=83385&idb=0

Дополнительная литература:

1. Криминология: Учебник для Вузов /Под ред. В.Н. Кудрявцева, В.Е. Эминова. –М.: Юристъ, 2005 –734с.

2. Шевцова К.А. Участие молодежи в преступлениях против общественного порядка : монография / К.А. Шевцова ; под ред. К.К. Панько. - Москва : Юстицинформ, 2024. - 148 с. - (Уголовное право). - Библиогр.: с. 140-147. - Библиогр. в подстр. примеч. - ISBN 978-5-6052226-0-6. - Текст : непосредственный.
https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=81153&idb=0

3. Русанов Г.А. Противодействие легализации (отмыванию) преступных доходов : учебное пособие для вузов / Г.А. Русанов. - Москва : Издательство Юрайт, 2021, 2024. - 157 с. - (Высшее образование). - Рекомендовано УМО ВО. - ISBN 978-5-534-03778-4. - Текст: непосредственный. https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=71583&idb=0

Программное обеспечение и электронные ресурсы:

1. СПС «КонсультантПлюс»; Система «ГАРАНТ».
2. www.zonazakona.ru.
3. www.sledovatel.ru;
4. www.crimescience.ru;
5. www.sartraccc.ru;
6. www.yurist.com.

V. 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.cons	Открытая лицензия для образовательных организаций

			ultant.ru	
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. Ельцина	сторонняя	https://www.prlib.ru	ФГБУ «Президентская библиотека имени Б. Н. 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, СУБД	Вид лицензирования
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).