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

Кафедра криминологии и уголовно-исполнительного права

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КИБЕРНЕТИЧЕСКАЯ ПРЕСТУПНОСТЬ

Б1.В.ДВ.04.02

год набора – 2023

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, очно-заочная, заочная
Квалификация:	магистр

Москва – 2023

Программа утверждена на заседании кафедры криминологии и уголовно-исполнительного права, протокол № 6 от «28» февраля 2023 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), 2023.

Программа составлена в соответствии с требованиями ФГОС ВО.

I. ОБЩИЕ ПОЛОЖЕНИЯ

I.1. Цели и задачи освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «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 (модуля) «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.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Кибернетическая преступность» относится к элективным дисциплинам (модулям) части, формируемой участниками образовательных отношений, Блока 1 (Б1.В.ДВ) основной профессиональной образовательной программы высшего образования.

Освоение дисциплины дает возможность расширения и углубления знаний, полученных на предшествующем этапе обучения, приобретения умений и навыков, определяемых содержанием программы. Компетенции, которые формируются в процессе освоения дисциплины, необходимы для успешной профессиональной деятельности. Обучающиеся приобретают способность самостоятельно находить и использовать необходимые содержательно-логические связи с другими дисциплинами программы, такими как «Теория квалификации преступлений», «Теория предупреждения преступности», «Фи-

нансовая преступность» и другими.

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

По итогам освоения дисциплины (модуля) обучающийся должен обладать следующими компетенциями в соответствии с ФГОС ВО:

Универсальные компетенции:

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

УК-2 Способен управлять проектом на всех этапах его жизненного цикла;

Профессиональные компетенции:

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.

Разделы (темы) дисциплины (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))**
Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК 1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними ИУК 1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению 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 ИУК 1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области
Понятие и виды кибернетической преступности	УК-2 Способен управлять проектом на всех этапах	ИУК 2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализа-

	его жизненного цикла	цию 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 ИУК 2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости ИУК 2.4 Разрабатывает план реализации проекта с использованием инструментов планирования ИУК 2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта
Личность киберпреступника	ПК-1 Способен разрабатывать нормативные правовые и локальные правовые акты в конкретных сферах юридической деятельности	ИПК 1.1 Определяет необходимость подготовки нормативных правовых актов и нормативных документов в сфере своей профессиональной деятельности и их отраслевую принадлежность ИПК 1.2 Применяет основные приемы законодательной техники при подготовке нормативных правовых актов в сфере своей профессиональной деятельности ИПК 1.3 Соблюдает правила юридической техники при подготовке нормативных документов в сфере своей профессиональной деятельности
Причины кибернетической преступности	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК 1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними ИУК 1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению 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 ИУК 1.5 Использует логико-методо-

		логический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области
Криминологическая характеристика хакерских атак	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК 1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними ИУК 1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению 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 ИУК 1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области
Кибернетическая преступность в зарубежных странах	ПК-5 Способен планировать и организовывать научные исследования, участвовать в научно-исследовательских работах по проблемам права; способен разрабатывать собственный научный проект	ИПК 5.1 Показывает способность проводить анализ и обобщение результатов научно-исследовательских работ с использованием современных достижений научного знания, передового отечественного и зарубежного опыта ИПК 5.2 Показывает способность участия в научно-исследовательской деятельности, сборе и первичной обработке эмпирической информации на основе использования современных методов и технологий обработки данных, средств вычислительной техники и коммуникаций, использования результатов научных исследований для подготовки аналитических записок, обзоров, отчетов и рекомендаций ИПК 5.3 Показывает способность определения и структурирования исследовательской проблемы в области профессиональной деятельности,

		аргументировать самостоятельный выбор, обосновать объект, предмет, цели, задачи и методы исследования по актуальной проблематике в профессиональной области и организационно обеспечить их реализацию
Предупреждение кибернетической преступности	УК-2 Способен управлять проектом на всех этапах его жизненного цикла	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 ИУК 2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости ИУК 2.4 Разрабатывает план реализации проекта с использованием инструментов планирования ИУК 2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта

В результате освоения дисциплины (модуля) «Кибернетическая преступность» обучающийся должен:

Наименование раздела дисциплины	**Планируемые результат обучения (знания, умения, владения)**
Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	**Обучающийся должен** **знать:** основные криминологические нормативные правовые акты против кибернетической преступности; правовое содержание регулирования информационно-телекоммуникационной деятельности, сущность основных понятий кибернетической преступности; основные виды рисков, связанных с компьютерной безопасностью предпринимательской деятельности и деятельностью граждан, в связи с использованием ими компьютеров**;** **уметь:** толковать различные юридические факты, правоприменительную и правоохранительную практику в сфере безопасной компьютерной деятельности; собирать и анализировать нормативную и фактической информацию, имеющую значение для изучения кибернетической преступности; осуществлять практическую информационно-поисковую и аналитическую деятельность по обеспечению

	компьютерной безопасности предпринимателей, граждан и должностных лиц; **владеть:** юридической терминологией; навыками квалифицированного составления локальных нормативных документов, обеспечивающих криминологическую компьютерную безопасность; выявлять, устранять и предупреждать причины и условия, способствующие совершению правонарушений и преступлений в области информационно-телекоммуникационной деятельности.
Понятие и виды кибернетической преступности	**Обучающий должен** **знать:** понятие и виды кибернетической преступности; законодательство по профилактике правонарушений и преступлений; особенности регламентирования профилактики правонарушений и преступлений в деятельности, связанной с использованием компьютеров; способы противодействия посягательствам на компьютерную безопасность предпринимателя, гражданина и должностного лица; **уметь:** анализировать статистические данные; предупреждать корпоративные конфликты; обеспечивать реализацию локальных правовых актов; критически анализировать свою работу, находить просчеты и ошибки, делать из них соответствующие выводы; выявлять и содействовать пресечению коррупционного поведения в области использования современных коммуникационных систем и компьютерных технологий; **владеть:** навыками анализа и обобщения получаемой информации, организации работы по обеспечению компьютерной безопасности; навыками наиболее целесообразного выбора линии поведения для эффективного, экономичного, законного ведения деятельности с использованием компьютеров.
Личность киберпреступника	**Обучающийся должен** **знать:** механизм формирования личности преступника; особенности поведения при совершении кибернетических преступлений; виды виктимологического поведения и значение его изучения; правовое обеспечение защиты предпринимателя и гражданина; **уметь:** предупреждать виктимологическое поведение предпринимателя и гражданина; обеспечивать защиту гражданина от компьютерных мошенничеств; выявлять причины и условия, способствовавшие совершению преступлений; обеспечивать реализацию актов применения права; критически анализировать свою работу, находить просчеты и ошибки, делать из них соответствующие выводы; выявлять и содействовать пресечению кибернетических преступлений; **владеть:** навыками анализа и обобщения получаемой информации, организации работы по обеспечению безопасности навыками наиболее целесообразного выбора линии поведения для эффективного, экономичного, законного ведения деятельности, связанной с использованием компьютеров.

Причины кибернетической преступности	**Обучающийся должен** **знать:** виды причин кибернетической преступности; опасность компьютерных мошенничеств и приемы защиты от них; способы взаимодействия с правоохранительными органами с целью противодействия кибернетической преступности; правила безопасной работы с коммуникационными системами; **уметь:** выявлять причины и условия, способствовавшие совершению кибернетических преступлений, и принимать необходимые меры по их устранению; определять критерии классификаций; применять правила детерминации к выявлению внутренних и внешних причин совершения компьютерных преступлений; **владеть:** навыками анализа и обобщения получаемой информации, организации работы по обеспечению безопасности; навыками наиболее целесообразного выбора линии поведения для эффективного, экономичного, законного осуществления деятельности, связанной с применением компьютеров; умением организовать работу по обеспечению безопасной работы на предприятии.
Криминологическая характеристика хакерских атак	**Обучающийся должен** **знать:** формы и виды хакерских атак и других видов компьютерных мошенничеств; формы и виды злоупотреблений должностными полномочиями и другие должностные преступления; виды коррупции, связанной с использованием компьютеров; другие формы коррупционного поведения, включая непотизм и фаворитизм; способы противодействия посягательствам на компьютерную безопасность предприятия и гражданина; **уметь:** выявлять причины и условия, способствовавшие совершению хакерских атак; выявлять взаимосвязь хакерской деятельности с должностными преступлениями; анализировать коррупционные риски и реализовывать управленческие антикоррупционные решения; осуществлять информационно-поисковую и аналитическую деятельность по выявлению признаков, свидетельствующих о посягательствах на компьютерную безопасность бизнеса и отдельного гражданина; выявлять и содействовать пресечению непотизма и фаворитизма; **владеть:** навыками анализа и обобщения получаемой информации; организовывать работу по обеспечению безопасности компьютерного поведения, как обычного человека, так и работника, и руководителя предприятия от мошеннических действий, с использованием компьютеров.
Кибернетическая преступность в зарубежных странах	**Обучающийся должен** **знать:** возможности и значение криминологической характеристики кибернетической преступности в зарубежных странах; способы взаимодействия предпринимателей и отдельных граждан с правоохранительными органами с целью противодействия посягательствам на коммуникационные сети и компьютерную безопасность предпринимательской деятельности и отдельных граждан за

	рубежом; правила отнесения стран к экономически развитым странам и к странам с переходной экономикой; **уметь:** принимать оптимальные управленческие решения при использовании компьютеров и коммуникационных сетей; выявлять причины и условия, способствовавшие совершению преступлений в этой области; анализировать и реализовывать управленческие инновации в профессиональной деятельности; осуществлять информационно-поисковую и аналитическую деятельность по выявлению признаков, свидетельствующих о посягательствах на компьютерную безопасность бизнеса; обеспечивать реализацию актов применения права; критически анализировать свою работу, находить просчеты и ошибки, делать из них соответствующие выводы; предупреждать правонарушения, связанные с использованием компьютеров; выявлять и устранять причины и условия, способствующие их совершению; **владеть:** навыками анализа и обобщения получаемой информации, организации работы по обеспечению компьютерной безопасности; навыками наиболее целесообразного выбора линии поведения для эффективного, экономичного, законного осуществления деятельности; связанной с использованием компьютеров, умением организовать работу по обеспечению компьютерной безопасности предприятия и обычного гражданина.
Предупреждение кибернетической преступности	**Обучающийся должен** **знать:** приемы и способы защиты от кибернетических преступлений; способы противодействия посягательствам на безопасность предприятия и гражданина; способы компьютерных мошенничеств и признаки, свидетельствующие о них; способы противодействия хакерским атакам; **уметь:** принимать оптимальные управленческие решения для предотвращения кибернетических преступлений, выявлять причины и условия, способствовавшие совершению компьютерных преступлений; анализировать и реализовывать управленческие инновации в профессиональной деятельности; осуществлять информационно-поисковую и аналитическую деятельность по выявлению признаков, свидетельствующих о посягательствах на компьютерную безопасность бизнеса; обеспечивать реализацию актов применения права; критически анализировать свою работу, находить просчеты и ошибки, делать из них соответствующие выводы; предупреждать правонарушения в области использования коммуникационных система, выявлять и устранять причины и условия, способствующие их совершению; выявлять и содействовать пресечению коррупционного поведения, связанного с использованием компьютеров; **владеть:** навыками анализа и обобщения получаемой информации; организовывать работу по обеспечению компьютерной безопасности предприятия и обычного гражданина.

II. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) «Кибернетическая преступность» составляет 3 з.е., 108 академических часов. Форма промежуточной аттестации – зачет.

2.1. Тематические планы

2.1.1. Тематический план для очной формы обучения

№ п/п	Раздел (тема) дисциплины (модуля)	семестр/триместр	Виды учебной деятельности и объем (в академических часах)				Технологии образовательного процесса	Формы текущего контроля / форма промежуточной аттестации
			Лекции	Практические занятия	Лабораторный практикум	СР		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	4	2			14	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эссе, реферат, коллоквиум
2	Понятие и виды кибернетической преступности	4		2		12	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	4		2		12	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
4	Причины кибернетической преступности	4		2		14	работа в малых группах, «займи позицию», разбор кон-	самостоятельная работа, эссе, реферат,

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

2.1.2. Тематический план для очно-заочной формы обучения

№ п/п	Раздел (тема) дисциплины (модуля)	семестр/триместр	Виды учебной деятельности и объем (в академических часах)				Технологии образовательного процесса	Формы текущего контроля / форма промежуточной аттестации
			Лекции	Практические занятия	Лабораторный практикум	СР		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической пре-	5	2			16	лекция-дискуссия, лекция-презентация, информационная,	самостоятельная работа, эссе, реферат, кол-

	ступностью						обобщающая, проблемная лекция	локвиум
2	Понятие и виды кибернетической преступности	5		2		12	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	5		2		12	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
4	Причины кибернетической преступности	5		2		12	работа в малых группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
5	Криминологическая характеристика хакерских атак	5		2		14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах	5		2		16	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум

7	Предупреждение кибернетической преступности	5			2	12	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	ВСЕГО		**2**	**10**	**2**	**94**		**Зачет**

2.1.3. Тематический план для заочной формы обучения

№ п/п	Раздел (тема) дисциплины (модуля)	курс	Виды учебной деятельности и объем (в академических часах)				Технологии образовательного процесса	Формы текущего контроля / форма промежуточной аттестации
			Лекции	Практические занятия	Лабораторный практикум	СР		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	2	2			12	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эссе, реферат, коллоквиум
2	Понятие и виды кибернетической преступности	2		2		14	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	2		2		12	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
4		2		2		14	работа в малых	самостоя-

	Причины кибернетической преступности						группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	тельная работа, эссе, реферат, коллоквиум
5	Криминологическая характеристика хакерских атак	2		2		12	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах	2				14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
7	Предупреждение кибернетической преступности	2			2	14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	ВСЕГО		**2**	**8**	**2**	**92**	**Зачет – 4 ак.ч.**	

Содержание дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Общая характеристика кибернетической преступности и взаимосвязь с экономи-	Особенности кибернетической преступности. Взаимосвязь с экономической преступностью. Уголовно-правовая характеристика компьютерных преступлений. Структура и характер кибернетической преступности. Виды латентной

	ческой преступностью	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 киберпреступника	Понятие и структура личности киберпреступника. Классификация и типология различных групп и типов киберпреступников. Механизм преступного поведения личности киберпреступника. 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 характеристика 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 ха-

		рактеристика 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

Наименование лекции	**Тематика лекции**	**Задания для подготовки к лекции**
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 кримино-	изучить и проанализировать: - нормативные акты в части правовой регламентации банковской деятельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой дея-

	логии 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.	тельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой деятельности.

2.3. Занятия практического типа

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

При освоении дисциплины (модуля) «Кибернетическая преступность» используются следующие виды самостоятельной работы обучающихся: 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 обучающихся применяются на всех формах обучения.

Темы коллоквиумов:

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.

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).

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 соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Университете имени О.Е. Кутафина (МГЮА) с целью фиксации результатов освоения модуля дисциплины преподаватель на последнем учебном занятии модуля проводит контрольную проверку уровня знаний обучающихся в формах, предусмотренных тематическим планом настоящей рабочей программы дисциплины (модуля) в качестве форм текущего контроля.

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.

21.Общая характеристика кибернетической преступности за рубежом.

22.Общая характеристика кибернетической преступности в других странах.

24.Соотношение кибернетической и организованной преступности.

25.Взаимосвязь экономических преступников и кибер-преступников.

26. Понятие, признаки и виды предупреждения кибернетической преступности.

27. Специальные субъекты предупреждения кибернетической преступности.

28. 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 (в действующей редакции) 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»//Собра-

ние 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. Постановление Правительства РФ от 14.09.2016 N 924 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (террито-

рий), 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.

25. 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.

26. 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).

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

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

Основная литература:

1. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с. — URL: https://urait.ru/bcode/467208

2. Русскевич, Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е.А. Русскевич. — Москва : ИНФРА-М, 2020. — 227 с. — URL: https://znanium.com/catalog/product/1061706

3. Мацкевич И.М. Причины экономической преступности. - М. : Проспект, 2017. – URL: http://ebs.prospekt.org/book/34334

Дополнительная литература:

1. Антонян Ю.М. Наука криминология : монография / Ю. М. Антонян. - М. : Юрлитинформ, 2015. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

2. Афанасьева, О. Р. Криминология : учебник и практикум для вузов / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. — Москва : Издательство Юрайт, 2020. — 360 с. — URL: https://urait.ru/bcode/454000

3. Бриллиантов А.В. Преступления в сфере экономической деятельности : учеб. пособие / Рос. гос. ун-т правосудия. - М. : РГУП, 2018. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

4. Гамза В.А. Безопасность коммерческого банка: организационно-правовые и криминалистические проблемы : монография / В. А. Гамза. - М. : Изд-ль Шумилова И.И., 2002. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

5. Гусейнов А.А. Меры профилактики и выявления киберпреступности в сети «интернет» / Гусейнов А.А., Подковка С.В. // Евразийский юридический журнал. - 2020. - № 3 (142). - С. 332-333. – URL: https://www.elibrary.ru/item.asp?id=42766210

6. Долженко Н.И. К вопросу о содержательных аспектах киберпреступности / Долженко Н.И., Хмелевская И.Г. // Nomothetika: Философия. Социология. Право. - 2020. - Т. 45. - № 2. - С. 315-322. – URL: https://www.elibrary.ru/item.asp?id=43931768

7. Захарова Л.И. Условия эффективного воздействия государства на теневую экономику : монография / Л. И. Захарова ; Междунар. ун-т природы, общества и человека "Дубна". Филиал "Протвино". - М. : Прометей, 2011. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

8. Ивличев П.С. Информационные технологии обеспечения безопасно-сти платежных средств в свете современных тенден-ций в киберпреступности / Ивличев П.С., Ивличева Н.А. // Экономика и предпринимательство. - 2017. - № 2-1 (79). - С. 135-139. – URL: https://www.elibrary.ru/item.asp?id=28790898

9. Козлова О.Е. Перспективы применения положительного опыта зарубежных стран в борьбе с киберпреступностью в Российской Федерации / Козлова О.Е., Самойлова А.В., Твердохлебова Э.В. // Актуальные научные исследования в современном мире. - 2020. - № 8-5 (64). - С. 42-47. – URL: https://www.elibrary.ru/item.asp?id=44003198

10. Криминалистическое обеспечение безопасности предпринимательской деятельности : научно-практическое пособие / О. Н. Васильева, Н. А. Иванов, М. В. Жижина и др. ; отв. ред. Е. П. Ищенко. – Москва : Проспект, 2018. — 192 с. - ISBN 978-5-392-28179-4. - URL: http://ebs.prospekt.org/book/40459

11. Кувшинова В.С. Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. - 2020. - № 5-4 (44). - С. 53-57. – URL: https://www.elibrary.ru/item.asp?id=42968917

12. Кучина Я.О. Криминалистические аспекты в уголовной политике: киберпреступность и тест Даубера // Вестник криминалистики. - 2020. - № 3 (75). - С. 48-54. – URL: https://www.elibrary.ru/item.asp?id=44146005

13. Лелюхин С.Е. Экономическая безопасность в предпринимательской

деятельности / Лелюхин С.Е., Коротченков А.М., Данилова У.В. - М. : Проспект, 2016. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

14. Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. - 2017. - N 5. - С. 19 - 29. – Режим доступа : СПС Консультант Плюс: \\consultant\Consultant\cons.exe, локальная сеть университета.

15. Магомедов Р.М. Анализ киберпреступности и борьба с ней // Экономика: вчера, сегодня, завтра. - 2020. - Т. 10. - № 6-1. - С. 48-54. – URL: https://www.elibrary.ru/item.asp?id=43983564

16. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 347 с. — URL: https://urait.ru/bcode/449839

17. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. - 2020. - № 1 (1). - С. 77-96. – URL: https://www.elibrary.ru/item.asp?id=44292184

18. Социальные отклонения / Кудрявцев В.Н., Бородин С.В., Нерсесянц В.С., Кудрявцев Ю.В. - М. : Юрид. Лит., 1989. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

19. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Издательство Юрайт, 2020. — 103 с. — URL: https://urait.ru/bcode/448300

20. Трофимцева С.Ю. Международное противодействие киберпреступности : сравнительный анализ рекомендаций Будапештской конвенции и законодательства снг в области уголовного права // Евразийский юридический журнал. - 2020. - № 8 (147). - С. 47-49. – URL: https://www.elibrary.ru/item.asp?id=44027644

21. Трофимцева С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности // Евразийский юридический журнал. - 2020. - № 10 (149). - С. 30-31. – URL: https://www.elibrary.ru/item.asp?id=44333053

22. Тюнин В.И. Преступления в сфере экономической деятельности : учеб.-практ. пособие / В. И. Тюнин. - М. : Юрлитинформ, 2012. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

23. Уголовно-юрисдикционная деятельность в условиях цифровизации : монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев [и др.]. - М. : ИзиСП : КОНТРАКТ, 2019. – Режим доступа : СПС Консультант Плюс: \\consultant\Consultant\cons.exe, локальная сеть университета.

24. Хачатрян А.К. Освобождение от уголовной ответственности за преступления в сфере экономической деятельности : дис. ... канд. юрид. наук : 12.00.08 : защищена 23.04.2015 / Хачатрян Артур Камович ; Университет имени О.Е. Кутафина (МГЮА). - М., 2014. - 168 с. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

25. Хутов К.М. Преступный монополизм: уголовно-политическое и

криминологическое исследование / К.М. Хутов ; отв. ред. сер. Н.А. Лопашенко. - М. : Волтерс Клувер, 2007. – Режим доступа : http://megapro.msal.ru/MegaPro/Web

26. Чабукиани О.А. Способы противодействия киберпреступности / Чабукиани О.А., Зорина Е.А., Солодовник В.В. // Социология и право. 2020. № 3 (49). С. 84-93. – URL: https://www.elibrary.ru/item.asp?id=44025033

27. Чекунов И.Г. Современное состояние киберпреступности в Российской Федерации / Чекунов И.Г., Шумов Р.Н. // Российский следователь. - 2016. - N 10. - С. 44 - 47. – Режим доступа : СПС Консультант Плюс: \\consultant\Consultant\cons.exe, локальная сеть университета.

28. Шайхаттарова С.В. Россия и международные стандарты по борьбе с киберпреступностью // Международное уголовное право и международная юстиция. - 2016. - N 4. - С. 26 - 29. – Режим доступа : СПС Консультант Плюс: \\consultant\Consultant\cons.exe, локальная сеть университета.

29. Шестак В.А. Унификация уголовного законодательства в сфере борьбы с киберпреступностью в странах-членах Европейского Союза / Шестак В.А., Адигамов А.И. // Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования. - 2020. - Т.2. - №1(2). – URL: https://www.elibrary.ru/item.asp?id=44173004

V. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

5.1. Обеспечение образовательного процесса иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса

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 имени О.Е. Кутафина (МГЮА), в том числе предоставление им общедоступной и персонализированной справочной, научной, образовательной, социальной информации посредством сервисов, функционирующих на основе прикладных информационных систем Университета имени О.Е. Кутафина (МГЮА).

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета имени О.Е. Кутафина (МГЮА). Помимо элек-

тронных библиотек Университета имени О.Е. Кутафина (МГЮА), он обеспечен индивидуальным неограниченным доступом ко всем удаленным электронно-библиотечным системам, базам данных и справочно-правовым системам, подключенным в Университете имени О.Е. Кутафина (МГЮА) 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 имени О.Е. Кутафина (МГЮА), так и вне ее.

Фонд электронных ресурсов Библиотеки включает следующие справочно-правовые системы, базы данных и электронные библиотечные системы:

5.1.1. Справочно-правовые системы:

1.	ИС «Континент»	сторонняя	http://continent-online.com	ООО «Агентство правовой интеграции «КОНТИНЕНТ», договоры: - № 18032020 от 20.03.2018 г. с 20.03.2018 г. по 19.03.2019 г.; - № 19012120 от 20.03.2019 г. с 20.03.2019 г. по 19.03.2020 г.; - № 20040220 от 02.03.2020 г. с 20.03.2020 г. по 19.03.2021 г. - №21021512 от 16.03.2021 г. с 20.03.2021 г. по 19.03.2022 г. - № 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.
2.	СПС Westlaw Academics	сторонняя	https://uk.westlaw.com	Филиал Акционерного общества «Томсон Рейтер (Маркетс) Юроп СА», договоры: - № 2TR/2019 от 24.12.2018 г. с 01.01.2019 г. по 31.12.2019 г.; - №RU03358/19 от 11.12.2019 г., с 01.01.2020 г. по 31.12.2020 г.; - № ЭБ-6/2021 от 06.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № 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.
3.	КонсультантПлюс	сторонняя		Открытая лицензия для образо-

			http://www.consultant.ru	вательных организаций
4.	Гарант	сторонняя	https://www.garant.ru	Открытая лицензия для образовательных организаций

5.1.2. Профессиональные базы данных:

3.	Коллекции полнотекстовых электронных книг информационного ресурса EBSCOHost БД eBook Collection	сторонняя	http:// web.a.ebscohost.com	ООО «ЦНИ НЭИКОН», договор № 03731110819000006 от 18.06.2019 г. бессрочно
4.	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)
5.	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
6.	НЭБ eLIBRARY.RU	сторонняя	http://elibrary.ru	ООО «РУНЕБ», договоры: - № SU-13-03/2019-1 от 27.03.2019 г. с 01.04.2019 г. по 31.03.2020 г.; - № ЭР-1/2020 от 17.04.2020 г. с 17.04.2020 г. по 16.04.2021 г.; - № ЭР-2/2021 от 25.03.2021 г. с 25.2021 г. по 24.03.2022 г.; - № 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.
7.	Legal Source			ООО «ЦНИ НЭИКОН», договоры:

		сторонняя	http://web.a.ebsco-host.com	- № 414-EBSCO/2020 от 29.11.2019 г., с 01.01.2020 г. по 31.12.2020 г.; - № ЭБ-5/2021 от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № ЭР-2/2022 от 01.10.2021 г., с 01.01.2022 г. по 31.12.2022 г.; - № 414- EBSCO/23 от 21.10.2022 г. с 01.01.2023 г. по 31.12.2023 г.
8.	ЛитРес: Библиотека	сторонняя	http://biblio.litres.ru	ООО «ЛитРес», договоры: - № 290120/Б-1-76 от 12.03.2020 г. с 12.03.2020 г. по 11.03.2021 г.; - № 160221/В-1-157 от 12.03.2021 г. с 12.03.2021 г. по 11.03.2022 г.; - № 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.

5.1.3. Электронно-библиотечные системы:

1.	ЭБС ZNANIUM.COM	сторонняя	http://znanium.com	ООО «Научно-издательский центр ЗНАНИУМ», договоры: - № 3489 бс от 14.12.2018 г. с 01.01.2019 г. по 31.12.2019 г.; - № 3/2019эбс от 29.11.2019 г. с 01.01.2020 г. по 31.12.2020 г.; - № 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.
2.	ЭБС Book.ru	сторонняя	http://book.ru	ООО «КноРус медиа», договоры: - № 18494735 от 17.12.2018 г. с 01.01.2019 г. по 31.12.2019 г.; - № ЭБ-2/2019 от 29.11.2019 г. с 01.01.2020 г. по 31.12.2020 г. - № ЭБ-4/2021 от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № 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.
3.	ВЧЗ РГБ (Виртуальный читальный зал Российской государственной библиотеки)	сторонняя	https://search.rsl.ru/	ФГБУ «Российская государственная библиотека», договор № 32312116538 от 14.02.2023 г. с 02.03.2023 г. по 01.03.2024 г.
4.	ЭБС Юрайт	сторонняя	http://www.biblio-online.ru	ООО «Электронное издательство Юрайт», договоры: -№ ЭБ-1/2019 от 01.04.2019 г. с 01.04.2019 г. по 31.03.2020 г.; - № ЭБ-1/2020 от 01.04.2020 г. с 01.04.2020 г. по 31.03.2021 г.

				- № ЭР-1/2021 от 23.03.2021 г. с 03.04.2021 г. по 02.04.2022 г.; - № 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.
5.	ЭБС «Юстицинформ»	сторонняя	https://elknigi.ru/	ООО «Юридический дом «Юстицинформ», договор № ЭР-1/2023 от 30.03.2023 г. с 05.04.2023 г. по 04.04.2024 г.
6.	ЭБС Проспект	сторонняя	http://ebs.prospekt.org	ООО «Проспект», договоры: -№ ЭБ-1/2019 от 03.07.2019 г. с 03.07.2019 г. по 02.07.2020 г; - № ЭБ-2/2020 от 03.07.2020 г. с 03.07.2020 г. по 02.03.2021 г.; - № 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.

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

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

№	Описание ПО	Наименование ПО, программная среда,	Вид лицензирования

		СУБД	
ПО, устанавливаемое на рабочую станцию			
1.	Операционная система	Windows 7	Лицензия
		Windows 10	Лицензия
		По договорам: № 32009118468 от 01.06.2020 г. № 31907826970 от 27.05.2019 г. № 31806485253 от 20.06.2018 г. №31705236597 от 28.07.2017 г. №31604279221 от 12.12.2016 г.	
2.	Антивирусная защита	Kaspersky Workspace Security	Лицензия
		По договорам: № 31907848213 от 03.06.2019 г. № 31806590686 от 14.06.2018 №31705098445 от 30.05.2017 № 31603346516 от 21.03.2016	
3.	Офисные пакеты	Microsoft Office	Лицензия
		По договорам: № 32009118468 от 01.06.2020 г. № 31907826970 от 27.05. 2019 г. № 31806485253 от 21.06.2018 г. №31705236597 от 28.07.2017 г. №31604279221 от 12.12.2016 г.	
4.	Архиваторы	7-Zip	Открытая лицензия
		WinRar	Открытая лицензия
5.	Интернет браузер	Google Chrome	Открытая лицензия
6.	Программа для просмотра файлов PDF	Adobe Acrobat reader	Открытая лицензия
		Foxit Reader	Открытая лицензия
7.	Программа для просмотра файлов DJVU	DjVu viewer	Открытая лицензия
8.	Пакет кодеков	K-Lite Codec Pack	Открытая лицензия
9.	Видеоплеер	Windows Media Player	В комплекте с ОС
		vlc pleer	Открытая лицензия
		flashpleer	Открытая лицензия
10.	Аудиоплеер	Winamp	Открытая лицензия
11.	Справочно- правовые системы (СПС)	Консультант плюс	Открытая лицензия
		Гарант	Открытая лицензия

Университет имени О.Е. Кутафина (МГЮА) располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам, и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

В реализации дисциплины (модуля) задействованы учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и поме-

щения для хранения и профилактического обслуживания учебного оборудования. Для проведения занятий лекционного типа обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, которые хранятся на электронных носителях.

5.3. Помещения для самостоятельной работы обучающихся

Помещения для самостоятельной работы обучающихся расположенные по адресу г. Москва ул. Садовая-Кудринская д.9 стр.1, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС Университета и включают в себя:

1. Электронный читальный зал на 135 посадочных мест:

– стол студенческий двухместный – 42 шт.,
– стол студенческий трехместный – 10 шт.,
– кресло для индивидуальной работы – 3 шт.,
– стул – 135 шт.,
– компьютер студенческий 50 MAC AB – 76 шт. (компьютерная техника подключена к сети «Интернет» и обеспечивает доступ в электронную информационно-образовательную среду),
– проектор с моторизованным лифтом Epson EB-1880 – 1 шт.,
– экран Projecta с электронным приводом – 1 шт.

Электронный читальный зал располагается на первом этаже, предназначенного для инвалидов и лиц с ограниченными возможностями здоровья, рабочие места в читальном зале оборудованы современными эргономичными моноблоками с качественными экранами, а также аудио гарнитурами.

Комплекс средств:

– рабочее место с увеличенным пространством – 2 шт.,
– наушники «накладного» типа – 1 компл.,
– лупа ручная для чтения 90mmx13.5mm – 1 шт.,
– линза Френеля в виниловой рамке 300*190 – 1 шт.

2. Читальные залы на 93 посадочных мест:

– стол студенческий двухместный – 24 шт.,
– стол студенческий трехместный – 2 шт.,
– кресло для индивидуальной работы – 7 шт.,
– стул – 93 шт.,
– компьютер студенческий 50 MAC AB – 11 шт.

3. Абонемент научной литературы на 4 посадочных мест:

– стол студенческий одноместный – 4 шт.,
– компьютер студенческий 50 MAC AB – 4 шт.,
– стул – 4 шт.

Помещение для самостоятельной работы обучающихся расположенное

по адресу г. Москва наб. Шитова д. 72 корп. 3, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС Университета и включает в себя:

- компьютер студенческий Lenovo – 16 шт.,
- стол студенческий одноместный – 16 шт.,
- стол студенческий двухместный – 17 шт.,
- стул – 42 шт.

Дисциплина (модуль) обеспечена помещениями для хранения и профилактического обслуживания учебного оборудования.