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

Кафедра уголовного права

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б1.В.ДВ.04.01

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 уголовного права, протокол № 11 от «30» марта 2023 года.

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

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

Русскевич Е.А.
Преступления против информационной безопасности: рабочая программа дисциплины (модуля) / Русскевич Е.А. — М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2023.

Программа составлена в соответствии с требованиями ФГОС ВО.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

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

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

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Преступления против информационной безопасности» (Б1.В.ДВ.04.01) 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», «Уголовно-правовое противодействие преступлениям против личности», «Уголовно-правовое противодействие преступлениям против собственности» и др.

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.

Профессиональные компетенции:

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

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

Разделы (темы) дисципли-	**Код и наименование**	**Индикатор достижения**

ны (модуля)	формируемых компетенций	компетенций (планируемый результат освоения дисциплины (модуля))
Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности Тема 1. Понятие и виды преступлений против информационной безопасности	**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
Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать	**ИПК 2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК 2.2** Понимает особенности различных форм реализации права **ИПК 2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение **ИПК 2.4** Определяет характер правоотношения и подлежащие применению нормы материального права **ИПК 2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права

	юридические консультации и заключения в различных сферах юридической деятельности	**ИПК 3.1** Выявляет и формулирует наличие правовой проблемы **ИПК 3.2** Знает и применяет правила оформления правового заключения и письменной консультации **ИПК 3.3** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Раздел II. Уголовно-правовая охрана информационной безопасности Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК 2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК 2.2** Понимает особенности различных форм реализации права **ИПК 2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение **ИПК 2.4** Определяет характер правоотношения и подлежащие применению нормы материального права **ИПК 2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права **ИПК 3.1** Выявляет и формулирует наличие правовой проблемы **ИПК 3.2** Знает и применяет правила оформления правового заключения и письменной консультации **ИПК 3.3** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Раздел II. Уголовно-правовая охрана информационной безопасности Тема 4. Преступления в сфере компьютерной информа-	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать	**ИПК 2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК 2.2** Понимает особенно-

ции: специальные правила квалификации	нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	сти различных форм реализации права **ИПК 2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение **ИПК 2.4** Определяет характер правоотношения и подлежащие применению нормы материального права **ИПК 2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права **ИПК 3.1** Выявляет и формулирует наличие правовой проблемы **ИПК 3.2** Знает и применяет правила оформления правового заключения и письменной консультации **ИПК 3.3** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Раздел II. Уголовно-правовая охрана информационной безопасности Тема 5. Лабораторный практикум	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права	**ИПК 2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК 2.2** Понимает особенности различных форм реализации права **ИПК 2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение **ИПК 2.4** Определяет характер правоотношения и подлежащие применению нормы материального права **ИПК 2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права

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

а) знать:

– российское уголовное законодательство о преступлениях против информационной безопасности;

– актуальные проблемы защиты информации уголовно-правовыми средствами;

– современные международные стандарты противодействия преступлениям против информационной безопасности;

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

б) уметь:

– правильно квалифицировать преступления в сфере компьютерной информации;

– правильно квалифицировать преступления в сфере оборота виртуальных активов;

– выявлять уголовно-правовые риски в информационной сфере;

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

– разрабатывать уголовно-правовые акты в области защиты компьютерной информации и цифровых ресурсов.

в) владеть:

– терминологией, связанной с уголовно-правовым противодействием угрозам информационной безопасности;

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

II. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) 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	Разделы (темы) дисциплины (модуля)	семестр/триместр	Виды учебной деятельности и объем (в академических часах)				Технология образовательного процесса	Форма текущего контроля/ Форма промежуточной аттестации
			лекции	практические занятия	лабораторный практикум	СР		
1	**Раздел I. Теорети-**	4	1			20	Лекция-	

	ческие основы уголовно-правовой охраны информационной безопасности Тема 1. Понятие и виды преступлений против информационной безопасности						дискуссия/ Проблемная лекция	
2	**Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности** Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности	4	1			22	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
3	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации	4		6		20	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
4	**Раздел II. Уголовно-правовая охрана информационной безопас-**			6		20	Коллоквиум, доклад с презента-	Тестирование/ устный и письмен-

	ности Тема 4. Преступления в сфере компьютерной информации: специальные правила квалификации						цией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	ный опрос/ контрольные задания
5	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 5. Лабораторный практикум	4			2	10	Доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
	Всего по ОФО		**2**	**12**	**2**	**92**	**Зачет**	

2.1.2. Тематический план для очно-заочной формы обучения

№ п/п	Разделы (темы) дисциплины (модуля)	семестр/ триместр	Виды учебной деятельности и объем (в академических часах)				Технология образовательного процесса	Форма текущего контроля/ Форма промежуточной аттестации
			лекции	практические занятия	лабораторный практикум	СР		
1	**Раздел I. Теоретические основы уголовно-правовой охраны**	4	1			20	Лекция-дискуссия/ Проблемная лекция	

	информационной безопасности Тема 1. Понятие и виды преступлений против информационной безопасности							
2	**Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности** Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности	4	1			22	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
3	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации	4		6		20	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
4	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 4. Преступления в сфере	4		4		22	Коллоквиум, доклад с презентацией, управляемая дис-	Тестирование/ устный и письменный опрос/ контроль-

	компьютерной информации: специальные правила квалификации						куссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	ные задания
5	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 5. Лабораторный практикум	4			2	10	Доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
	Всего по ОЗФО		**2**	**10**	**2**	**94**	**Зачет**	

2.1.3. Тематический план для заочной формы обучения

№ п/п	Разделы (темы) дисциплины (модуля)	Курс	Виды учебной деятельности и объем (в академических часах)				Технология образовательного процесса	Форма текущего контроля/ Форма промежуточной аттестации
			лекции	практические занятия	лабораторный практикум	СР		
1	**Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности**	2	1			17	Лекция дискуссия/ Проблемная лекция	

	Тема 1. Понятие и виды преступлений против информационной безопасности **(установочная сессия)**							
2	**Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности** Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности **(установочная сессия)**	2	1			17	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
3	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации	2		4		20	Коллоквиум, доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
4	**Раздел II. Уголовно-правовая охрана информационной безопасности**	2		4	2	20	Коллоквиум, доклад с презентацией, управля-	Тестирование/ устный и письменный опрос/

	Тема 4. Преступления в сфере компьютерной информации: специальные правила квалификации						емая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	контрольные задания
5	**Раздел II. Уголовно-правовая охрана информационной безопасности** Тема 5. Лабораторный практикум	2			2	18	Доклад с презентацией, управляемая дискуссия, кейс-стади, мозговой штурм, работа в малых группах, написание эссе/реферата, составление схем	Тестирование/ устный и письменный опрос/ контрольные задания
Итого:			**2**	**8**	**2**	**58**	**Зачет – 4 ак.ч.**	
	Всего по ЗФО		**2**	**8**	**2**	**92**	**4**	

Содержание дисциплины (модуля)

Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности

Тема 1. Понятие и виды преступлений против информационной безопасности

1. Понятие информационной безопасности в современном мире.
2. Социальная обусловленность уголовно-правовой охраны информационной безопасности.
3. Основные подходы к определению преступлений против информационной безопасности.
4. Виды преступлений против информационной безопасности. Преступления против информационной безопасности в широком и узком смысле. Компьютерные и компьютеризированные преступления. Цифровая экономи-

ка как самостоятельный объект уголовно-правовой охраны. Криптовалютные преступления.

Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности

1. Международно-правовые основы обеспечения информационной безопасности.
2. Ответственность за посягательства на информационную безопасность по законодательству зарубежных стран.

Раздел II. Уголовно-правовая охрана информационной безопасности

Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации

1. Понятие и виды преступлений в сфере компьютерной информации.
2. Особенности законодательного определения преступлений в сфере компьютерной информации.
3. Общие правила квалификации преступлений в сфере компьютерной информации (по признакам состава преступления).

Тема 4. Преступления в сфере компьютерной информации: специальные правила квалификации

1. Квалификация преступлений в сфере компьютерной информации с учетом межотраслевых связей.
2. Квалификация неоконченных преступлений в сфере компьютерной информации.
2. Квалификация преступлений в сфере компьютерной информации, совершенных в соучастии.
3. Квалификация сложных единичных преступлений в сфере компьютерной информации и их отграничение от множественности.
4. Квалификация преступлений в сфере компьютерной информации при конкуренции уголовно-правовых норм.

2.2. Занятия лекционного типа

Раздел I. Теоретические основы уголовно-правовой охраны информационной безопасности

Тема 1. Понятие и виды преступлений против информационной безопасности

Содержание:

1. Понятие информационной безопасности в современном мире. Цифровая экономика как самостоятельный объект уголовно-правовой охраны.
2. Социальная обусловленность уголовно-правовой охраны информационной безопасности.
3. Основные подходы к определению преступлений против информационной безопасности.
4. Виды преступлений против информационной безопасности. Преступления против информационной безопасности в широком и узком смысле.
5. Компьютерные и компьютеризированные преступления.
6. Криптовалютные преступления.

Задание для подготовки:

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

Тема 2. Международно-правовые основы и зарубежный опыт противодействия преступлениям против информационной безопасности

Содержание:

1. Международно-правовые основы обеспечения информационной безопасности.
2. Ответственность за посягательства на информационную безопасность по законодательству стран Содружества Независимых Государств.
3. Ответственность за посягательства на информационную безопасность по законодательству Китайской Народной Республики.
4. Ответственность за посягательства на информационную безопасность по законодательству стран Европейского Союза.
5. Ответственность за посягательства на информационную безопасность по законодательству Великобритании, Сингапура и США.

Задание для подготовки:

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

2.3. Занятия семинарского типа

Раздел II. Уголовно-правовая охрана информационной безопасности

Тема 3. Преступления в сфере компьютерной информации: особенности законодательного определения и общие правила квалификации

1. Понятие и виды преступлений в сфере компьютерной информации.
2. Особенности законодательного определения преступлений в сфере компьютерной информации.
3. Квалификация преступлений в сфере компьютерной информации по признакам объекта.
4. Квалификация преступлений в сфере компьютерной информации по признакам объективной стороны.
5. Квалификация преступлений в сфере компьютерной информации по признакам субъекта.
6. Квалификация преступлений в сфере компьютерной информации по признакам субъективной стороны.

Задания для подготовки:

1. Изучить нормативные материалы и основную литературу, указанные в Списке литературы и нормативного материала раздела «Учебно-методическое обеспечение» рабочей программы. Рекомендуется ознакомиться с дополнительной литературой.
2. Составить схему по вопросу: «Общественно опасные последствия преступлений в сфере компьютерной информации (на основе анализа признаков ст. 272-274^2 УК)».
3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Предмет неправомерного доступа к компьютерной информации», «Уголовно-правовая охрана критической информационной инфраструктуры Российской Федерации: фьюжн-норма УК РФ», «Использование вредоносной компьютерной программы и пентест: вопросы юридической оценки», «Должностное лицо как субъект преступлений в сфере компьютерной информации: правила квалификации (на основе анализа судебной практики)».
4. Обобщить судебную практику по вопросам темы.
5. Составить 2-3 казуса по теме.

Тема 4. Преступления в сфере компьютерной информации: специальные правила квалификации

1. Квалификация преступлений в сфере компьютерной информации с учетом межотраслевых связей.
2. Квалификация неоконченных преступлений в сфере компьютерной информации.
2. Квалификация преступлений в сфере компьютерной информации, совершенных в соучастии.

3. Квалификация сложных единичных преступлений в сфере компьютерной информации и их отграничение от множественности.

4. Квалификация преступлений в сфере компьютерной информации при конкуренции уголовно-правовых норм.

Задания для подготовки:

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

2. Составить схему по вопросу: «Конкуренция уголовно-правовых норм о преступлениях в сфере компьютерной информации».

3. Подготовить доклады с презентациями (с их последующим обсуждением) по темам: «Юридический и фактический моменты окончания преступлений в сфере компьютерной информации», «Нетипичные аспекты соучастия в компьютерных преступлениях», «Компьютерные преступления и криптовалютные преступления», «Компьютерные преступления и хищения, совершаемые в системах дистанционного банковского обслуживания: правила квалификации (на основе анализа судебной практики)».

4. Обобщить судебную практику по вопросам темы.

5. Составить 2-3 задачи по теме.

Лабораторный практикум

Фабула задачи № 1:

19-летний Выжанов решил отомстить старосте группы Афанасьевой, которая ранее сообщила в деканат о неподобающем поведении Выжанова на занятиях. С этой целью он привлек своих приятелей 21-летнего Попова и 15-летнего Уланцева. Выжанов объяснил, что необходимо устроить «кибертравлю» Афанасьевой: взломать ее аккаунты в социальных сетях и электронную почту, выложить в групповом чате компрометирующие сведения об Афанасьевой. На телефон Афанасьевой постоянно с разных номеров отправлять угрозы и сообщения оскорбительного характера. Выжанов вовлек еще троих однокурсников, которые также пожелали поучаствовать в «наказании» старосты. В течение месяца группа под руководством Выжанова смогла взломать все известные аккаунты Афанасьевой, на них они размещали материалы экстремистского и порнографического характера. В общий чат студентов Университета была выложена личная переписка Афанасьевой, в которой она обсуждала преподавателей и студентов (иногда в неприличной форме). От старосты отвернулись друзья и однокурсники, обсуждался вопрос об ее отчислении из вуза. Не выдержав «кибертравли» Афанасьева, вернувшись домой, приняла большую дозу снотворного. Благодаря действиям брата Афанасьевой, который своевременно вызвал медицинскую помощь, ее жизнь была спасена.

Вопросы для обсуждения:

1. Дайте уголовно-правовую оценку содеянного.

2. Определите предмет преступления.

3. Влияет ли групповой способ совершения преступления на квалификацию содеянного?

4. Возможно ли привлечение указанных в задаче лиц к ответственности по ст. 110 УК «Доведение до самоубийства»?

Фабула задачи № 2:

Петюшов и Волобуев осуществили неправомерный доступ к учетным записям пользователей «wmalliance» и «Djin37», после чего изменили их учетную информацию, добавив свой уникальный идентификационный номер для общения в реальном времени, а также от имени пользователей «wmalliance» и «Djin37» создали тему «Вывод BTC-e / Биткоинов. +7%», и положительные комментарии к ней от имени других неустановленных пользователей сайта. После чего Петюшов и Волобуев, ввели в заблуждение Вишневского, пообещав ему обменять «BTC-e» код на российские рубли, чего заведомо не намеревались делать. Вишневский, будучи введенным в заблуждение, используя свою учетную запись «ser198», с целью обмена, принадлежащего ему «BTC-e» кода на 10 000 долларов США на российские рубли, в личном сообщении передал пользователю «wmalliance», доступ к которому имели Петюшов и Волобуев, «BTC-e» код на 10 000 долларов США, рыночная стоимость которого, по состоянию на дату отправки сообщения, согласно заключению эксперта, составляла 821 100 рублей 00 копеек. Далее Петюшов и Волобуев зачислили полученный BTC-e код, принадлежащий потерпевшему, на счет своей учетной записи, и в дальнейшем распорядились им по своему усмотрению.

Вопросы для обсуждения:

1. Дайте уголовно-правовую оценку содеянного.

2. Определите предмет преступления.

3. Влияет ли групповой способ совершения преступления на квалификацию содеянного?

Фабула задачи № 3:

Работник Новороссийского морского порта Горохов решил посмотреть личную электронную почту на служебном компьютере. В почтовом ящике он обнаружил письмо с предложением о трудоустройстве в международной торговой компании. Горохов нажал на содержащуюся в электронном письме вредоносную ссылку, начался процесс загрузки, а потом его компьютер оказался заблокирован, на экране появилось сообщение на английском языке. В течение считанных минут вредоносная программа смогла проникнуть в системы управления технологическим процессом передачи грузов. Вирус также проник в отслеживающие и контролирующие перевалку грузов АСУ ТП и зашифровал файлы, критически важные для технологических процессов. За-

шифрованные системы напрямую повлияли на «всю корпоративную IT-сеть объекта (за пределами зоны обслуживания объекта) и системы управления камерами, а также привели к потере систем контроля и управления критическими процессами морского порта. В результате инцидента в течение 30 часов все операции на объекте были остановлены.

Вопросы для обсуждения:

1. Дайте уголовно-правовую оценку содеянного.

2. Определите предмет преступления.

Количество задач, их условия и вопросы для обсуждения определяются преподавателем для каждой группы обучающихся.

Методические рекомендации для подготовки к лабораторному практикуму:

В ходе решения задачи обучающийся должен проанализировать фактические обстоятельства, дать им юридическую оценку, правильно квалифицировать преступление, определить соответствующие уголовно-правовые, правильно их истолковать и юридически грамотно сформулировать решение данного казуса. Одновременно с этим рассмотреть связанные с содержанием задачи теоретические положения уголовного права, позволяющие разрешить конкретную ситуацию. Действуя подобным образом, обучающийся должен научиться тесно увязывать теорию уголовного права с практикой применения действующего уголовного законодательства и таким путем полнее и глубже постичь суть уголовно-правовых категорий, понятий, раскрыть и уяснить социальный смысл и служебную роль применяемых в данной ситуации норм уголовного права, понятий, уголовно-правовых конструкций. Обучающиеся обязаны в процессе подготовки к практическим занятиям решать задачи письменно в особой тетради. В письменном виде решение должно содержать краткое изложение фактических обстоятельств, их оценку, указание на нормы уголовного права и при необходимости на положения нормативных правовых актов других отраслей права, в соответствии с которыми решена задача. Конечный вывод по задаче может быть сформулирован в виде резолютивной части решения суда, заключения прокурора, юрисконсульта. Пользуясь письменным текстом, обучающийся в своем выступлении на занятиях должен дать развернутое юридическое обоснование принятого решения. Решение задачи в виде ссылки только на норму права недопустимо.

2.4. Самостоятельная работа

Виды самостоятельной работы:

1. Изучение законодательства, основной и дополнительной литературы по темам занятий лекционного и семинарского типа.

2. Подготовка к занятиям семинарского типа включает следующие типы самостоятельной работы обучающегося по любой форме обучения:

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

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

– обобщение судебной практики по вопросам темы практического занятия;

– составление 2-3 казусов на основе обобщенной судебной практики с последующим их решением на занятиях семинарского типа.

Модельные задания для обучающихся всех форм обучения:

1. Изложение материала по отдельным вопросам, указанным к каждой теме практического занятия, в виде схемы с последующим ее обсуждением в ходе практического занятия с целью выявления достоинств и недостатков

2. Каждый обучающийся в течение семестра должен подготовить как минимум один доклад с презентацией во вопросам, сформулированным к темам занятий семинарского типа, и после его обсуждения в ходе практического занятия представить преподавателю грамотно оформленные тезисы доклада (5-6 страниц, кегль шрифта основного текста 14 пт., междустрочный интервал – полуторный) и презентацию. Тезисы доклада должны иметь необходимый научный аппарат (правильно оформленные ссылки на источники). В докладе должны быть рассмотрены дискуссионные точки зрения по сложным и актуальным вопросам выбранной темы, юридически грамотно сформулирована и обоснована точка зрения автора. При подготовке доклада необходимо использовать специальную литературу по теме (монографии, научные публикации в периодических изданиях). Докладчик должен быть готов отстаивать свою позицию в ходе обсуждения доклада.

3. Сбор, анализ и обобщение судебной практики с использованием сайта Росправосудие – https://rospravosudie.com и сайта Судебные и нормативные акты РФ – http://sudact.ru.

4. Составление казуса (задачи) на основе изученных уголовных дел в рамках обобщения судебной практики. С этой целью необходимо выбирать наиболее интересные решения судов по конкретным делам.

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с п. 2.10 Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный юридический университет 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, зафиксированных в методических материалах по проведению текущего контроля успеваемости обучающихся указанные в столбце «Формы текущего контроля» тематического плана.

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

Промежуточная аттестация проводится в виде решения кейс-стади.

Вопросы для подготовки к промежуточной аттестации:

1. Информационная безопасность как объект уголовно-правовой охраны.
2. Виды преступлений против информационной безопасности. Преступления против информационной безопасности в широком и узком смысле.
3. Компьютерные и компьютеризированные преступления.
4. Криптовалютные преступления.
5. Международно-правовые основы обеспечения информационной безопасности.
6. Ответственность за посягательства на информационную безопасность по законодательству стран Содружества Независимых Государств.
7. Ответственность за посягательства на информационную безопасность по законодательству Китайской Народной Республики.
8. Ответственность за посягательства на информационную безопасность по законодательству стран Европейского Союза.
9. Ответственность за посягательства на информационную безопасность по законодательству Великобритании, Сингапура и США.
10. Понятие и виды преступлений в сфере компьютерной информации.
11. Особенности законодательного определения преступлений в сфере компьютерной информации.
12. Неправомерный доступ к компьютерной информации.
13. Создание, использование и распространение вредоносных компьютерных программ.
14. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
15. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
16. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.
17. Квалификация преступлений в сфере компьютерной информации по признакам объекта.
18. Квалификация преступлений в сфере компьютерной информации

по признакам объективной стороны.

19. Квалификация преступлений в сфере компьютерной информации по признакам субъекта.

20. Квалификация преступлений в сфере компьютерной информации по признакам субъективной стороны.

21. Квалификация преступлений в сфере компьютерной информации с учетом межотраслевых связей.

22. Квалификация неоконченных преступлений в сфере компьютерной информации.

23. Квалификация преступлений в сфере компьютерной информации, совершенных в соучастии.

24. Квалификация сложных единичных преступлений в сфере компьютерной информации и их отграничение от множественности.

25. Квалификация преступлений в сфере компьютерной информации при конкуренции уголовно-правовых норм.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

4.1. Нормативные правовые акты (в действующей редакции)

1. Конституция Российской Федерации, принятая народным голосованием 12 декабря 1993 г. – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_34481/

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_34661/

4.2. Судебная практика

1. Постановления Пленума Верховного суда РФ. – URL: http://www.vsrf.ru/documents/own/, http://www.consultant.ru/.

2. Сборник постановлений Пленумов Верховных Судов СССР, РСФСР и РФ по уголовным делам : сборник / составители А. И. Рарог, А. А. Бимбинов. — 3-е изд. — Москва : Проспект, 2019. — 784 с. — ISBN 978-5-392-28463-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/150857

3. Судебная практика по конкретным делам: сайт Судебные и нормативные акты РФ. – URL: http://sudact.ru

4.3. Основная литература

1. Корабельников С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476798 (дата обращения: 18.02.2023). – Режим доступа: локальная сеть Университета имени О.Е. Кутафина (МГЮА).

2. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. — М.: ИНФРА-М, 2023. – 351 с. – URL: https://znanium.com/catalog/document?id=415589 (дата обращения: 17.02.2023). – Режим доступа: локальная сеть Университета имени О.Е. Кутафина (МГЮА).

3. Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учеб. пособие / Е.А. Русскевич. – 2-е изд., доп. — М.: ИНФРА-М, 2019. – 188 с. – (Высшее образование: Магистратура). – URL: http://znanium.com/catalog/product/979195 (дата обращения: 17.02.2023). – Режим доступа: локальная сеть Университета имени О.Е. Кутафина (МГЮА).

4. Уголовное право зарубежных стран в 3 т. Том 3. Особенная часть: учебник для бакалавриата и магистратуры / отв. ред. Н. Е. Крылова. 5-е изд., перераб. и доп. М.: Издательство Юрайт, 2017. – 397 с. URL: https://biblio-online.ru/book/E58E2F3E-E4F2-4C48-BFE4-B50C9327A324/ugolovnoe-pravo-zarubezhnyh-stran-v-3-t-tom-1-obschaya-chast-angliya-ssha (дата обращения: 19.02.2023). – Режим доступа: локальная сеть Университета имени О.Е. Кутафина (МГЮА).

5. Уголовное право России. Части Общая и Особенная : учебник / под ред. А. И. Рарога. — 10-е изд., перераб. и доп. — Москва : Проспект, 2020. — 944 с. - ISBN 9785392300181 ; [Электронный ресурс]. - URL: http://ebs.prospekt.org/book/40435

6. Юрченко И. А. Преступления против информационной безопасности: учебное пособие. — Москва: Проспект, 2021. — 208 с. - ISBN 978-5-392-33751-4; [Электронный ресурс]. - URL: http://ebs.prospekt.org/book/44295

4.4. Дополнительная литература:

1. Воронин В. Н. Уголовно-правовые риски развития цифровых технологий: постановка проблемы и методы научного исследования // Вестник Университета имени О.Е. Кутафина. – 2018. – № 12. – С. 73-80. – URL: https://www.elibrary.ru/item.asp?id=36991705&ysclid=lf8qa6a1nz881766466

2. Русскевич Е.А. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / Е.А. Русскевич, И.Г. Чекунов // Уголовное право. – 2022. – № 5. – С. 26-35. – URL: https://www.elibrary.ru/item.asp?edn=aghwvk

3. Русскевич Е.А. Нарушение правил эксплуатации средств хране-

ния, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации / Е.А. Русскевич // Уголовное право. – 2020. – № 5. – С. 94-104. – URL: https://www.elibrary.ru/item.asp?id=44836976

4. Русскевич Е.А. О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения / Е.А. Русскевич // Российское правосудие. – 2019. – № 2. – С. 35-41. – URL: https://www.elibrary.ru/item.asp?id=36761575

5. Русскевич Е.А. О некоторых аспектах квалификации соучастия в преступлениях в сфере компьютерной информации / Е.А. Русскевич // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2019. – № 3 (57). – С. 30-34. – URL: https://www.elibrary.ru/item.asp?id=41338186

6. Русскевич Е.А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации / Е.А. Русскевич, А.Ю. Решетников // Уголовное право. – 2018. – № 2. – С. 86-95. – URL: https://www.elibrary.ru/item.asp?id=34968309

7. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е.А. Русскевич // Международное уголовное право и международная юстиция. – 2018. – № 3. – С. 10-13. – URL: https://www.elibrary.ru/item.asp?id=35040412

8. Юрченко И.А. Кибербезопасность как объект преступления // Судья. – 2016. – № 4 (64). – С. 50-52. – URL: https://elibrary.ru/item.asp?id=30040549

9. Юрченко И.А. Сталкер как субъект уголовной ответственности // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2018. – № 12. – С. 53-61. – URL: https://elibrary.ru/item.asp?id=36991703

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

5.1.2. Профессиональные базы данных:

1.	Web of Science	сторонняя	https://apps.webofknowledge.com	ФГБУ «Государственная публичная научно-техническая библиотека России», сублицензионные договоры: - № WOS/668 от 02.04.2018 г.; - № WOS/349 от 05.09.2019 г.; ФГБУ «Российский фонд фундаментальных исследований» (РФФИ), сублицензионные договоры: - № 20-1566-06235 от 22.09.2020 г.; - № 21-1706-06235 от 14.07.2021 г.
2.	Scopus	сторонняя	https://www.scopus.com	ФГБУ «Государственная публичная научно-техническая библиотека России», сублицензионные договоры: - № SCOPUS/668 от 09 января 2018 г.; - № SCOPUS/349 от 09 октября 2019 г.; ФГБУ «Российский фонд фундаментальных исследований» (РФФИ), сублицензионные договоры: - № 20-1573-06235 от 22.09.2020 г.;

				- № 21-1702-06235 от 14.07.2021 г.
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: - № 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

		сторонняя	http://web.a.ebsco-host.com	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.

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 дисциплине (модулю)

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

№	Описание ПО	Наименование ПО, программная среда, СУБД	Вид лицензирования
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.	
4.	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	
5.	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.	
7.	Архиваторы	7-Zip	Открытая лицензия
		WinRar	Открытая лицензия
8.	Интернет браузер	Google Chrome	Открытая лицензия
9.	Программа для просмотра файлов PDF	Adobe Acrobat reader	Открытая лицензия
		Foxit Reader	Открытая лицензия
10.	Программа для просмотра файлов DJVU	DjVu viewer	Открытая лицензия
11.	Пакет кодеков	K-Lite Codec Pack	Открытая лицензия
12.	Видеоплеер	Windows Media Player	В комплекте с ОС
		vlc pleer	Открытая лицензия
		flashpleer	Открытая лицензия
13.	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 помещения 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.