Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный университет им. А.Н. Косыгина
(Технологии. Дизайн. Искусство)»

Институт «Академия имени Маймонида»
Кафедра Уголовного права и адвокатуры

РАБОЧАЯ ПРОГРАММА

Теория и практика обеспечения кибербезопасности

Уровень образования	*бакалавриат*
Направление	код наименование 40.03.01 Юриспруденция
Направленность	наименование *Уголовно-правовой профиль*
Срок освоения образовательной программы по очной форме обучения	*4 года*
Форма(-ы) обучения	*очная*

Рабочая программа *учебной дисциплины Теория и практика обеспечения кибербезопасности* основной профессиональной образовательной программы высшего образования, рассмотрена и одобрена на заседании кафедры, протокол № 6 от 21.02.2023 г.

Разработчик(и) рабочей программы *учебной дисциплины/учебного модуля:*

1. *Профессор* *Лебедев Семен Яковлевич*

Заведующий кафедрой: *С.Я. Лебедев*

1. ОБЩИЕ СВЕДЕНИЯ

*Учебная дисциплина/учебный модуль «*Теория и практика обеспечения кибербезопасности*»* изучается в шестом семестре.

Курсовая работа/Курсовой проект – не предусмотрен(а)

1.1. Форма промежуточной аттестации:

шестой семестр - *зачет*

1.2. Место *учебной дисциплины* в структуре ОПОП

Учебная дисциплина Теория и практика обеспечения кибербезопасности относится к части программы Элективные дисциплины 3.

Основой для освоения *дисциплины* являются результаты обучения по предшествующим дисциплинам и практикам:

- *Теория государства и права;*
- *Уголовное право. Общая часть.*
- *Криминология*

Результаты обучения по *учебной дисциплине*, используются при изучении следующих дисциплин и прохождения практик:

- *Уголовное право. Особенная часть.*
- *Основы национальной безопасности.*

Результаты освоения *учебной дисциплины* в дальнейшем будут использованы при прохождении *производственной* практики и (или) выполнении выпускной квалификационной работы.

2. ЦЕЛИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Целями освоения дисциплины «Теория и практика обеспечения кибербезопасности» являются:

- формирование у студентов системных, профессиональных знаний о сущности и особенностях кибербезопасности, теоретических и практических основах ее обеспечения, роли в научном и практическом обеспечении общественного порядка, общественной безопасности и предупреждения правонарушений, тенденциях современного развития;

- изучение нормативных правовых документов, законов и подзаконных актов необходимых для познания системы кибербезопасности, теоретических основ и практических направлений ее обеспечения, предупреждения правонарушений, совершаемых в киберпространстве и под влиянием киберпространства, развитие умений использования теоретического знания в практике предупреждения правонарушений, совершаемых в киберпространстве и под влиянием киберпространства, и обеспечении кибербезопасности;

- формирование у обучающихся компетенции(-й), установленной(-ых) образовательной программой в соответствии с ФГОС ВО по данной дисциплине/модулю;

Результатом обучения по учебной дисциплине «Теория и практика обеспечения кибербезопасности» является овладение обучающимися знаниями, умениями, навыками и опытом деятельности, характеризующими процесс формирования компетенций и обеспечивающими достижение планируемых результатов освоения учебной дисциплины.

2.1. Формируемые компетенции, индикаторы достижения компетенций, соотнесённые с планируемыми результатами обучения по *дисциплине*:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по *дисциплине/модулю***
ПК-7 *Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства*	*ИД-ПК-7.1.* *Использование в условиях нарушения прав, свобод и законных интересов физических, должностных и юридических лиц, механизмов защиты граждан, субъектов общественных отношений*	*- Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства* *- Способен к использованию в условиях нарушения прав, свобод и законных интересов физических, должностных и юридических лиц, механизмов защиты граждан, субъектов общественных отношений* *- Способен к использованию научных знаний и применение законодательства о противодействии преступности, а также выявление и использование в профессиональной деятельности положительный правоприменительный опыт правоохранительных органов и судов* *- Способен к выявлению отношения сторон к ходу и результатам процедуры медиации*
	ИД-ПК-7.2. *Использование научных знаний и применение законодательства о противодействии преступности, а также выявление и использование в профессиональной деятельности положительный правоприменительный опыт правоохранительных органов и судов*	
	ИД-ПК-7.3. *- Выявление отношения сторон к ходу и результатам процедуры медиации*	

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоёмкость учебной дисциплины по учебному плану составляет:

по очной форме обучения –	3	**з.е.**	108	**час.**

3.1. Структура учебной дисциплины для обучающихся по видам занятий *(очная форма обучения)*

Структура и объем дисциплины

Объем дисциплины по семестрам	форма промежуточной аттестации	всего, час	Контактная аудиторная работа, час				Самостоятельная работа обучающегося, час		
			лекции, час	практические занятия, час	лабораторные занятия, час	практическая подготовка, час	*курсовая работа/ курсовой проект*	самостоятельная работа обучающегося, час	промежуточная аттестация, час
6 семестр	Зачет	108	16	28				64	
Всего:		108	16	28				64	

3.2. Структура учебной дисциплины для обучающихся по разделам и темам дисциплины: (очная форма обучения)

Планируемые (контролируемые) результаты освоения: код(ы) формируемой(ых) компетенции(й) и индикаторов достижения компетенций	Наименование разделов, тем; форма(ы) промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	*Лабораторные работы/ индивидуальные занятия час*	Практическая подготовка час		
	***Шестой* семестр**						
ПК-7 *ИД-ПК-7.1;* *ИД-ПК-7.2;* *ИД-ПК-7.3*	Теоретические и правовые основы безопасности личности, общества, государства. Право и безопасность в эпоху шестого технологического уклада.	+	+			+	
	Понятие кибербезопасности. Цели, задачи, функции кибербезопасности. Кибербезопасность в системе национальной и общественной безопасности.	+	+			+	Формы текущего контроля: *1. устный опрос.* *2. тестирование.*
	Национально-правовые и международно-правовые основы обеспечения кибербезопасности.	+	+			+	
	Понятие угроз кибербезопасности. Угрозы кибербезопасности в системе угроз национальной и общественной безопасности.	+	+			+	
	Система кибербезопасности. Субъекты и объекты кибербезопасности: правовые, организационные и информационно-технологические ресурсы.	+	+			+	
	Практическое обеспечение кибербезопасности. Междисциплинарные ресурсы практического обеспечения кибербезопасности.	+	+			+	
	Взаимодействие государственных и негосударственных структур в системе обеспечения кибербезопасности.	+	+			+	
	Состояние и перспективы международного сотрудничества в обеспечении кибербезопасности.	+	+			+	
	И Т О Г О	16	28			64	*зачет проводится в устной форме, собеседование*

3.3. Краткое содержание *учебной дисциплины*

№ пп	Наименование раздела и темы дисциплины	Содержание раздела (темы)
Тема 1.	Теоретические и правовые основы безопасности личности, общества, государства. Право и безопасность в эпоху шестого технологического уклада.	Понятие, основные признаки, ресурсы шестого технологического уклада, его влияние на общественные отношения и их безопасное состояние. Гибридный мир, его формирование, развитие и социально-правовые последствия. Цифровой мир, его социально-правовые угрозы и последствия. Право безопасности и его место в системе российского права. Правовые основы безопасности личности, общества, государства. Опасности и безопасность в эпоху шестого технологического уклада, их отражение в правоотношениях. Трансформация и модернизация современных и будущих правоотношений. Инновационное право и инновационные правоотношения в эпоху шестого и последующих технологических укладов.
Тема 2.	Понятие кибербезопасности. Цели, задачи, функции кибербезопасности. Кибербезопасность в системе национальной и общественной безопасности.	Понятие киберпространства как источника социальных опасностей и безопасности. Опасности, угрозы, риски и вызовы киберпространства, их социально-правовая оценка. Понятие кибербезопасности. Соотношение опасностей и безопасности в киберпространстве, механизмы их взаимосвязи и взаимодействия. Цели, задачи, функции кибербезопасности. Оценка предпосылок, условий и гарантий обеспечения кибербезопасности. Место и роль кибербезопасности в системе национальной и общественной безопасности. Соотношение и взаимовлияние кибербезопасности и иных видов безопасности в системе общественных отношений.
Тема 3.	Национально-правовые и международно-правовые основы обеспечения кибербезопасности.	Федеральное законодательство о кибербезопасности, его конституционно-правовые, информационно-правовые, гражданско-правовые, административно-правовые, уголовно-правовые и иные правовые ресурсы. Международно-правовой потенциал кибербезопасности, имплементация норм международного законодательства о кибербезопасности в российском праве. Региональные (в т.ч., муниципальные), отраслевые и ведомственные правовые ресурсы кибербезопасности. Правовая оценка пробелов и издержек современного законодательства о кибербезопасности, условия, гарантии и перспективы их

		устранения и нейтрализации.
Тема 4.	Понятие угроз кибербезопасности. Угрозы кибербезопасности в системе угроз национальной и общественной безопасности.	Понятие и признаки угроз кибербезопасности. Цифровые и иные информационно-технологические источники угроз кибербезопасности. Искусственный интеллект как источник угроз безопасности. Угрозы кибербезопасности как общественно вредные и общественно опасные деяния. Виды и формы угроз кибербезопасности. Киберпреступность как угроза кибербезопасности. Место и роль киберпреступности в системе угроз кибербезопасности. Понятие и виды киберпреступлений, их уголовно-правовая оценка и квалификация. Криминологическая характеристика киберпреступлений. Состояние, уровень, динамика, структура и характер киберпреступности. Криминологическая оценка личности киберпреступника и виктимологическая оценка жертвы киберпреступления. Механизмы совершения киберпреступлений. Угрозы кибербезопасности в системе угроз национальной и общественной безопасности. Взаимосвязь и взаимообусловленность киберугроз, киберпреступлений и иных традиционных уголовно-наказуемых деяний.
Тема 5.	Система кибербезопасности. Субъекты и объекты кибербезопасности: правовые, организационные и информационно-технологические ресурсы.	Понятие и признаки системы кибербезопасности. Виды подсистем кибербезопасности, их взаимосвязь и взаимообусловленность. Условия и гарантии системности обеспечения кибербезопасности. Субъекты и объекты кибербезопасности. Государственные и негосударственные, специализированные и неспециализированные субъекты кибербезопасности. Правоохранительные органы в системе обеспечения кибербезопасности. Частные структуры в системе обеспечения кибербезопасности. Оценка кадрового профессионального ресурса в обеспечении кибербезопасности. Киберпространство, киберпреступность, ее причины, условия, киберпреступники, потенциальные и реальные потерпевшие от киберпреступлений как объекты кибербезопасности. Правовые, организационные, информационно-технологические и иные ресурсы обеспечения кибербезопасности. Место и роль субъектов кибербезопасности в системе обеспечения национальной и общественной безопасности.
Тема 6.	Практическое обеспечение кибербезопасности. Междисциплинарные ресурсы практического обеспечения кибербезопасности.	Понятие и признаки профессиональной деятельности по обеспечению кибербезопасности. Основные направления обеспечения кибербезопасности: безопасность критической инфраструктуры, сетевая безопасность, когнитивная безопасность, безопасность приложений, облачная безопасность, информационная безопасность, цифровая безопасность, аварийное восстановление, безопасность хранения, мобильная безопасность, иные виды и формы обеспечения кибербезопасности. Предупреждение киберпреступлений и форензика в системе обеспечения кибербезопасности. Междисциплинарный подход к оценке и обеспечению кибербезопасности. Оценка состояния кибербезопасности. Международный, федеральный, региональный, отраслевой и персональный уровни обеспечения кибербезопасности.
Тема 7.	Взаимодействие государственных и негосударственных структур в системе обеспечения кибербезопасности.	Понятие, организационно-правовые основы и формы взаимодействия государственных и негосударственных, специализированных и неспециализированных структур в системе обеспечения кибербезопасности. Основные принципы взаимодействия государственных и негосударственных структур в системе обеспечения кибербезопасности. Организация и

		обеспечение взаимодействия субъектов кибербезопасности. Условия и гарантии успешного взаимодействия субъектов в системе обеспечения кибербезопасности.
Тема 8.	Состояние и перспективы международного сотрудничества в обеспечении кибербезопасности.	Понятие, организационно-правовые основы и формы международного сотрудничества в системе обеспечения кибербезопасности. Современная социально-правовая оценка международного сотрудничества в обеспечении кибербезопасности. Основные принципы международного сотрудничества в обеспечении кибербезопасности. Организация и формы международного сотрудничества в обеспечении кибербезопасности. Условия и гарантии успешного международного сотрудничества в обеспечении кибербезопасности.

3.4. Организация самостоятельной работы обучающихся

Самостоятельная работа студента – обязательная часть образовательного процесса, направленная на развитие готовности к профессиональному и личностному самообразованию, на проектирование дальнейшего образовательного маршрута и профессиональной карьеры.

Самостоятельная работа обучающихся по дисциплине организована как совокупность аудиторных и внеаудиторных занятий и работ, обеспечивающих успешное освоение дисциплины.

Аудиторная самостоятельная работа обучающихся по дисциплине выполняется на учебных занятиях под руководством преподавателя и по его заданию. Аудиторная самостоятельная работа обучающихся входит в общий объем времени, отведенного учебным планом на аудиторную работу, и регламентируется расписанием учебных занятий.

Внеаудиторная самостоятельная работа обучающихся – планируемая учебная, научно-исследовательская, практическая работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия, расписанием учебных занятий не регламентируется.

Внеаудиторная самостоятельная работа обучающихся включает в себя:

- *подготовку к лекциям, практическим и зачету;*
- *изучение учебных пособий;*
- *изучение теоретического и практического материала по рекомендованным источникам;*
- *выполнение домашних заданий;*
- *подготовка рефератов и докладов, эссе;*
- *подготовка к коллоквиуму;*
- *выполнение индивидуальных заданий;*
- *подготовка к промежуточной аттестации в течение семестра;*

Самостоятельная работа обучающихся с участием преподавателя в форме иной контактной работы предусматривает групповую и (или) индивидуальную работу с обучающимися и включает в себя:

- *проведение консультаций перед зачетом по необходимости;*
- *проведение ежегодного конкурса работ студентов на тему: «Развитие теории и практики обеспечения кибербезопасности».*
- *консультации по организации самостоятельного изучения отдельных разделов/тем, базовых понятий учебных дисциплин профильного/родственного*

бакалавриата, которые формировали ОПК и ПК, в целях обеспечения преемственности образования;

Перечень разделов/тем/, полностью или частично отнесенных на самостоятельное изучение с последующим контролем:

№ пп	Наименование раздела /темы *дисциплины/модуля,* выносимые на самостоятельное изучение	Задания для самостоятельной работы	Виды и формы контрольных мероприятий (учитываются при проведении текущего контроля)	Трудоемкость, час
Тема.	*Теоретические и правовые основы безопасности личности, общества, государства. Право и безопасность в эпоху шестого технологического уклада.*	*1. Подготовка к устному опросу*	*устное собеседование*	8
Тема.	*Понятие кибербезопасности. Цели, задачи, функции кибербезопасности. Кибербезопасность в системе национальной и общественной безопасности.*	*1.Подготовка к устному опросу*	*устное собеседование*	6

3.3. Применение электронного обучения, дистанционных образовательных технологий

При реализации программы учебной дисциплины электронное обучение и дистанционные образовательные технологии не применяются.

1. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО *ДИСЦИПЛИНЕ*, КРИТЕРИИ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ, СИСТЕМА И ШКАЛА ОЦЕНИВАНИЯ

1.1. Соотнесение планируемых результатов обучения с уровнями сформированности компетенций.

Уровни сформированности компетенции(-й)	**Итоговое количество баллов в 100-балльной системе по результатам текущей и промежуточной аттестации**		**Оценка в пятибалльной системе по результатам текущей и промежуточной аттестации**	**профессиональной(-ых) компетенции(-й)** *ИД-ПК-7.1;* *ИД-ПК-7.2;* *ИД-ПК-7.3*
высокий			Зачтено (отлично)	*Обучающийся уверенно:* *- Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства* *- Способен к использованию в условиях нарушения прав, свобод и законных интересов физических, должностных и юридических лиц, механизмов защиты граждан, субъектов общественных отношений* *- Способен к использованию научных знаний и применение законодательства о противодействии преступности, а также*

				выявление и использование в профессиональной деятельности положительный правоприменительный опыт правоохранительных органов и судов *- Способен к выявлению отношения сторон к ходу и результатам процедуры медиации*
повышенный			Зачтено (хорошо)	*Обучающийся достаточно:* *- Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства* *- Способен к использованию в условиях нарушения прав, свобод и законных интересов физических, должностных и юридических лиц, механизмов защиты граждан, субъектов общественных отношений* *- Способен к использованию научных знаний и применение законодательства о противодействии преступности, а также выявление и использование в профессиональной*

				деятельности положительный правоприменительный опыт правоохранительных органов и судов *- Способен к выявлению отношения сторон к ходу и результатам процедуры медиации*
базовый			Зачтено (удовлетворительно)	*Обучающийся со значительными затруднениями:* *- Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства* *- Способен к использованию в условиях нарушения прав, свобод и законных интересов физических, должностных и юридических лиц, механизмов защиты граждан, субъектов общественных отношений* *- Способен к использованию научных знаний и применение законодательства о противодействии преступности, а также выявление и использование в профессиональной*

				деятельности положительный правоприменительный опыт правоохранительных органов и судов *- Способен к выявлению отношения сторон к ходу и результатам процедуры медиации*
низкий			Не зачтено (неудовлетворительно)	

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ, ВКЛЮЧАЯ САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

При проведении контроля самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации по *учебной дисциплине Теория и практика обеспечения кибербезопасности* проверяется уровень сформированности у обучающихся компетенций и запланированных результатов обучения по дисциплине, указанных в разделе 2 настоящей программы.

2.1. Формы текущего контроля успеваемости, примеры типовых заданий:

№ пп	Формы текущего контроля	Примеры типовых заданий
	Устный опрос по темам	**Тема 2. Понятие кибербезопасности. Цели, задачи, функции кибербезопасности. Кибербезопасность в системе национальной и общественной безопасности.** 1. Дайте понятие киберпространства. 2. Оцените позитивные и негативные последствия функционирования киберпреострвнства. 3. Определите признаки опасностей, угроз, рисков и вызовов киберпространства. 4. Дайте определение кибербезопасности. 5. Оцените, как соотносятся между собой опасности и безопасность в киберпространстве. 6. Перечислите задачи и функции кибербезопасности. 7. Определите место и роль кибербезопасности в системе национальной и общественной безопасности. 8. Обоснуйте соотношение и взаимовлияние кибербезопасности и иных видов безопасности в системе общественных отношений.

№ пп	Формы текущего контроля	Примеры типовых заданий
	Тестирование по темам	**Тема 6. Практическое обеспечение кибербезопасности. Междисциплинарные ресурсы обеспечения кибербезопасности.** Вопрос 1. Безопасность критической инфраструктуры – это: А) безопасность государства от критики оппозиционных структур. Б) защита информационных ресурсов, похищение которых может негативно отразиться на деятельности органов государственной власти. В) защита компьютерных систем, сетей и других активов, о которой зависит экономическое благополучие, национальная и общественная безопасность государства. Г) обеспечение информационной безопасности технико-технологической инфраструктуры предприятия. Д) защита приоритетных ресурсов субъекта хозяйственной деятельности от информационных атак. Вопрос 2. Фишинг – это: А) хитрый прием ловли на удочку крупной рыбы с использованием интернета. Б) похищение крупных денежных средств со счетов высокооплачиваемых сотрудников частных компаний. В) мошеннические манипуляции со счетами финансовых компаний. Г) вид интернет-мошенничества, направленного на получение доступа к конфиденциальным данным пользователей – логинам и паролям. Д) обман покупателей и заказчиков. Вопрос 3. Кибербуллинг – это А) мошенническая киберигра с шарами на основе правил игры в боуллинг для вымогательства денег. Б) издевательство над человеком, психологическая травля с использованием интернет-технологий. В) использование интернета для организации мошеннических действий. Г) мошеннический прием в социальных сетях, направленный на знакомство с человеком для выманивания у него денежных средств. Д) вид интернет-мошенничества, направленного на получение доступа к конфиденциальным данным Вопрос 4. Форензика – это: А) основанная на искусственном интеллекте методика исследования цифровых источников

№ пп	Формы текущего контроля	Примеры типовых заданий
		информации о киберугрозах. Б) поиск и фиксация угроз кибербезопасности. В) методика изобличения киберпреступников в совершении ими мошеннических манипуляций с финансовыми средствами. Г) наука о раскрытии и расследовании преступлений, связанных с компьютерной информацией. Д) криминалистическая теория о кибербезопасности. Вопрос 5. Какой федеральный закон содержит правовую регламентацию устранения из интернет-пространства сюжетов, содержащих признаки киберпреступления: А) Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности". Б) Закон РФ от 11 марта 1992 г. N 2487-I "О частной детективной и охранной деятельности в Российской Федерации". В) Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". Г) Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Д) Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

2.2. Критерии, шкалы оценивания текущего контроля успеваемости:

Наименование оценочного средства (контрольно-оценочного мероприятия)	**Критерии оценивания**	**Шкалы оценивания**	
		100-балльная система	**Пятибалльная система**
Устный опрос	*Ответ дан полностью. Нет ошибок в логических рассуждениях. Возможно наличие одной неточности, не являющиеся следствием незнания или непонимания учебного материала. Обучающийся показал полный объем знаний, умений в освоении пройденных тем и применение их на практике*		*5*
	Ответ дан полностью. Допущена одна ошибка или два-три недочета.		*4*

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	Ответ дан не полностью. Допущены грубые ошибки.		*3*
	Ответ не дан		*2*
Реферат	*Обучающийся, в процессе подготовки реферата продемонстрировал глубокие знания дисциплины, сущности проблемы, были даны логически последовательные, содержательные, полные, правильные и конкретные исследования выбранной темы; даны рекомендации по использованию данных в будущем для аналогичных ситуаций.*		*5*
	Обучающийся, в процессе подготовки реферата продемонстрировал глубокие знания дисциплины, сущности проблемы, были даны логически последовательные, содержательные, исследования выбранной темы; даны рекомендации по использованию данных в будущем для аналогичных ситуаций, однако, имеются незначительные неточности, представлен недостаточно полный объем исследования выбранной темы.		*4*
	Обучающийся слабо ориентируется в материале, не раскрывает суть проблемы и не предлагает конкретного ее решения. *Обучающийся не принимал активного участия в работе группы, выполнившей задание на «хорошо» или «отлично».*		*3*
	Обучающийся не раскрыл исследуемую тему и продемонстрировал низкий уровень теоретических знаний.		*2*
Письменный отчет с результатами выполненных практических заданий	*Работа выполнена полностью. Нет ошибок в логических рассуждениях. Возможно наличие одной неточности или описки, не являющиеся следствием незнания или непонимания учебного материала. Обучающийся показал полный объем знаний, умений в освоении пройденных тем и применение их на практике.*		*5*
	Работа выполнена полностью, но обоснований шагов решения недостаточно. Допущена одна ошибка или два-три недочета.		*4*

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания		
		100-балльная система	Пятибалльная система	
	Допущены более одной ошибки или более двух-трех недочетов.		*3*	
	Работа выполнена не полностью. Допущены грубые ошибки.		*2*	
Тест	*За выполнение каждого тестового задания испытуемому выставляются баллы. Номинальная шкала предполагает, что за правильный ответ к каждому заданию выставляется один балл, за не правильный — ноль. В соответствии с номинальной шкалой, оценивается всё задание в целом, а не какая-либо из его частей.* *В заданиях с выбором нескольких верных ответов, заданиях на установление правильной последовательности, заданиях на установление соответствия, заданиях открытой формы используют порядковую шкалу. В этом случае баллы выставляются не за всё задание, а за тот или иной выбор в каждом задании, например, выбор варианта, выбор соответствия, выбор ранга, выбор дополнения. В соответствии с порядковой шкалой за каждое задание устанавливается максимальное количество баллов, например, три. Три балла выставляются за все верные выборы в одном задании, два балла - за одну ошибку, один - за две ошибки, ноль — за полностью неверный ответ.* *Правила оценки всего теста:* *общая сумма баллов за все правильные ответы составляет наивысший балл, например, 20 баллов. В спецификации указывается общий наивысший балл по тесту.* *Также устанавливается диапазон баллов, которые необходимо набрать для того, чтобы получить отличную, хорошую, удовлетворительную или неудовлетворительную оценки.* *Рекомендуемое процентное соотношение баллов и оценок по пятибалльной системе. Например:* *«2» - равно или менее 40%* *«3» - 41% - 64%* *«4» - 65% - 84%*		*5*	*85% - 100%*
			4	*65% - 84%*
			3	*41% - 64%*
			2	*40% и менее 40%*

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания		
		100-балльная система	Пятибалльная система	
	«5» - 85% - 100%			

2.3. Промежуточная аттестация:

Форма промежуточной аттестации	Типовые контрольные задания и иные материалы для проведения промежуточной аттестации:
Зачет *в устной форме, собеседование*	

2.4. Критерии, шкалы оценивания промежуточной аттестации учебной дисциплины/модуля:

Форма промежуточной аттестации Наименование оценочного средства	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
Зачет: *устный опрос*	*Обучающийся знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.*		*зачтено*
	НАПРИМЕР: *Обучающийся не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.*		*не зачтено*

2.5. Система оценивания результатов текущего контроля и промежуточной аттестации.

Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.

Форма контроля	100-балльная система	Пятибалльная система
Текущий контроль:		
- опрос		*2 – 5*
- тестирование		*2 – 5*
- письменный отчет с результатами выполненных практических заданий		*2 – 5*
- реферат		*2 – 5*
Промежуточная аттестация *Зачет с оценкой (устный опрос)*		*зачтено* *не зачтено*
Итого за семестр *зачёт с оценкой*		

Полученный совокупный результат конвертируется в пятибалльную систему оценок в соответствии с таблицей:

100-балльная система	пятибалльная система	
	зачет с оценкой/экзамен	**зачет**
	отлично зачтено (отлично)	зачтено
	хорошо зачтено (хорошо)	
	удовлетворительно зачтено (удовлетворительно)	
	неудовлетворительно	не зачтено

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Реализация программы предусматривает использование в процессе обучения следующих образовательных технологий:

- *проблемная лекция;*
- *проектная деятельность;*
- *проведение интерактивных лекций;*
- *групповых дискуссий;*
- *ролевых игр;*
- *тренингов;*
- *анализ ситуаций и имитационных моделей;*
- *преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, в том числе с учётом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей;*
- *поиск и обработка информации с использованием сети Интернет;*
- *дистанционные образовательные технологии;*
- *применение электронного обучения;*
- *просмотр учебных фильмов с их последующим анализом;*
- *использование на лекционных занятиях видеоматериалов и наглядных пособий;*
- *самостоятельная работа в системе компьютерного тестирования;*
- *обучение в сотрудничестве (командная, групповая работа);*

– *технологии с использованием игровых методов: ролевых, деловых, и других видов обучающих игр;*

4. ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Практическая подготовка в рамках *учебной дисциплины* реализуется при проведении *практических занятий,* связанных с будущей профессиональной деятельностью.

5. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной аттестации.

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения.

Учебные и контрольно-измерительные материалы представляются в формах, доступных для изучения студентами с особыми образовательными потребностями с учетом нозологических групп инвалидов:

Для подготовки к ответу на практическом занятии, студентам с ограниченными возможностями здоровья среднее время увеличивается по сравнению со средним временем подготовки обычного студента.

Для студентов с инвалидностью или с ограниченными возможностями здоровья форма проведения текущей и промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины. При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся создаются, при необходимости, фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ *ДИСЦИПЛИНЫ*

Характеристика материально-технического обеспечения дисциплины составляется в соответствии с требованиями ФГОС ВО.

Материально-техническое обеспечение *дисциплины* при обучении с использованием традиционных технологий обучения.

Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.	**Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.**

Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.	Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.
115035, г. Москва, ул. Садовническая, д. 52/45	
учебные аудитории №101, 102, 106, 107 для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации направлений юриспруденция и психология	комплект учебной мебели, *доска меловая* технические средства обучения, служащие для представления учебной информации большой аудитории: – *ноутбук,* – *проектор,* специализированное оборудование: *наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочей программе дисциплины.*
Помещения для самостоятельной работы обучающихся	**Оснащенность помещений для самостоятельной работы обучающихся**
читальный зал библиотеки:	*компьютерная техника;* *подключение к сети «Интернет»*

Материально-техническое обеспечение *учебной дисциплины/учебного модуля* при обучении с использованием электронного обучения и дистанционных образовательных технологий.

Необходимое оборудование	Параметры	Технические требования
Персональный компьютер/ ноутбук/планшет, камера, микрофон, динамики, доступ в сеть Интернет	Веб-браузер	Версия программного обеспечения не ниже: Chrome 72, Opera 59, Firefox 66, Edge 79, Яндекс.Браузер 19.3
	Операционная система	Версия программного обеспечения не ниже: Windows 7, macOS 10.12 «Sierra», Linux
	Веб-камера	640x480, 15 кадров/с
	Микрофон	любой
	Динамики (колонки или наушники)	любые
	Сеть (интернет)	Постоянная скорость не менее 192 кБит/с

Технологическое обеспечение реализации программы/модуля осуществляется с использованием элементов электронной информационно-образовательной среды университета.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ/УЧЕБНОГО МОДУЛЯ

Информационное обеспечение дисциплины в разделах 10.1 и 10.2 формируется на основании печатных изданий, имеющихся в фонде библиотеки, и электронных ресурсов, к которым имеет доступ Университет. Сайт библиотеки ***http://biblio.kosygin-rgu.ru*** *(см. разделы «Электронный каталог» и «Электронные ресурсы»).*

Печатные издания и электронные ресурсы, которые не находятся в фонде библиотеки и на которые Университет не имеет подписки, в разделах 10.1 и 10.2 не указываются.

В разделе 10.3 Таблицы перечисляются методические материалы (указания, рекомендации и т.п.) для обучающихся по освоению дисциплины, в том числе по самостоятельной работе, имеющиеся в библиотеке в электронном или бумажном формате.

Методические материалы (указания, рекомендации и т.п.), не зарегистрированные в РИО, отсутствующие в библиотеке, но размещенные в электронной информационно-образовательной среде (ЭИОС), могут быть включены в раздел 10.3 таблицы с указанием даты утверждения на заседании кафедры и номера протокола.

Например:

№ п/п	Автор(ы)	Наименование издания	Вид издания (учебник, УП, МП и др.)	Издательство	Год издания	Адрес сайта ЭБС или электронного ресурса *(заполняется для изданий в электронном виде)*	Количество экземпляров в библиотеке Университета
10.1 Основная литература, в том числе электронные издания							
1	Джафарли В.Ф. Криминология кибербезопасности: в 5 т. / под ред. С.Я. Лебедева.	Т. 1: Криминологическая кибербезопасность: теоретические, правовые и технологические основы Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности Т. 3: Криминологические средства предупреждения преступности в сфере информационно-	Монографическая серия	Москва: Проспект	2021-2022		10

		коммуникационных технологий Т. 4: Формирование и развитие междисциплинарного правового ресурса обеспечения криминологической кибербезопасности Т. 5: Криминологическая кибербезопасность: перспективы развития					
10.2 Дополнительная литература, в том числе электронные издания							
10.3 Методические материалы (указания, рекомендации по освоению дисциплины (модуля) авторов РГУ им. А. Н. Косыгина)							

8. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

8.1. Ресурсы электронной библиотеки, информационно-справочные системы и профессиональные базы данных:

Информация об используемых ресурсах составляется в соответствии с Приложением 3 к ОПОП ВО.

№ пп	Электронные учебные издания, электронные образовательные ресурсы
1.	*ЭБС «Лань» http://www.e.lanbook.com/*
2.	*«Znanium.com» научно-издательского центра «Инфра-М» http://znanium.com/*
3.	*Электронные издания «РГУ им. А.Н. Косыгина» на платформе ЭБС «Znanium.com» http://znanium.com/*
4.	…
	Профессиональные базы данных, информационные справочные системы
1.	…
2.	…
3.	…

8.2. Перечень программного обеспечения

Перечень используемого программного обеспечения с реквизитами подтверждающих документов составляется в соответствии с Приложением № 2 к ОПОП ВО.

№п/п	Программное обеспечение	Реквизиты подтверждающего документа/ Свободно распространяемое
1.	*Windows 10 Pro, MS Office 2019*	*контракт № 18-ЭА-44-19 от 20.05.2019*
2.	*PrototypingSketchUp: 3D modeling for everyone*	*контракт № 18-ЭА-44-19 от 20.05.2019*
3.	*V-Ray для 3Ds Max*	*контракт № 18-ЭА-44-19 от 20.05.2019*
4.	...	
5.	...	...

ЛИСТ УЧЕТА ОБНОВЛЕНИЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ/МОДУЛЯ

В рабочую программу учебной дисциплины/модуля внесены изменения/обновления и утверждены на заседании кафедры:

№ пп	год обновления РПД	характер изменений/обновлений с указанием раздела	номер протокола и дата заседания кафедры

9.