

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»**

Юридический факультет

УТВЕРЖДЕНО
решением Ученого совета ННГУ
протокол № 10 от 02.12.2024 г.

Рабочая программа дисциплины

Международное и внутригосударственное регулирование
информационной безопасности

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
40.03.01 - Юриспруденция

Направленность образовательной программы
Правовое обеспечение международных коммуникаций

Форма обучения
очная

г. Нижний Новгород

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.08.01 Международное и внутригосударственное регулирование информационной безопасности относится к части, формируемой участниками образовательных отношений образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

| Формируемые компетенции (код, содержание компетенции) | Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции | | Наименование оценочного средства | |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------|
| | Индикатор достижения компетенции (код, содержание индикатора) | Результаты обучения по дисциплине | Для текущего контроля успеваемости | Для промежуточной аттестации |
| УК-5: Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах | <p>УК-5.1: Использует знания об историческом наследии и социокультурных традиций различных социальных групп, опирающиеся на знание этапов исторического развития России в контексте мировой истории и ряда культурных традиций мира, включая мировые религии, философские и этические учения</p> <p>УК-5.2: Учитывает особенности межкультурного взаимодействия на основе использования основных философских идей и категорий, с учетом исторического развития и социально-этического контекста</p> <p>УК-5.3: Находит способы преодоления коммуникативных барьеров при межкультурном взаимодействии, в том числе при конфликтной ситуации</p> <p>УК-5.4: Придерживается принципов недискриминационного взаимодействия, определяет цели и задачи</p> | <p>УК-5.1:</p> <p>Знать: особенности межкультурного взаимодействия, обусловленные разнообразием общества.</p> <p>Уметь: учитывать особенности межкультурного взаимодействия, обусловленные различием этических, религиозных и ценностных систем</p> <p>Владеть: навыками межкультурного взаимодействия, в условиях различия этических, религиозных и ценностных систем.</p> <p>УК-5.2:</p> <p>Знать: основные философские идеи и категории, обеспечивающие межкультурное взаимодействие.</p> <p>Уметь: использовать основные философские идеи и категории при межкультурном взаимодействии</p> <p>Владеть: Навыками использования основных философских идей и категорий при межкультурном</p> | <p>Кейс-задача</p> <p>Тест</p> | <p>Зачёт:</p> <p>Контрольные вопросы</p> |

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------------------------------|
| | <p>межкультурного профессионального взаимодействия в условиях различных этнических, религиозных ценностных систем</p> | <p>взаимодействии</p> <p>УК-5.3: Знать: причины и типы коммуникативных барьеров в межкультурном взаимодействии. Уметь: выявлять возможные причины коммуникативных барьеров в межкультурном взаимодействии Владеть: навыками преодоления коммуникативных барьеров в межкультурном взаимодействии</p> <p>УК-5.4: Знать: принципы недискриминационного взаимодействия при межкультурном профессиональном взаимодействии. Уметь: применять принципы недискриминационного взаимодействия при межкультурном профессиональном взаимодействии Владеть: навыками принципов недискриминационного взаимодействия при межкультурном профессиональном взаимодействии</p> | | |
| <p>ПК МП-5: Способен представлять интересы физических и юридических лиц в судах, международной и национальной юстиции</p> | <p>ПК МП-5.1: Анализирует ситуацию с точки зрения нарушения норм отечественного и международного права ПК МП-5.2: Готовит текст юридических документов для обращения в судебные инстанции ПК МП-5.3: Поддерживает позицию стороны в устном разбирательстве</p> | <p>ПК МП-5.1: Знать: Конституцию РФ, законодательство РФ, систему источников международного права, место норм международного права в правовой системе РФ Уметь: анализировать конкретную ситуацию с точки зрения нарушения норм отечественного и международного права Владеть: навыками анализа отечественного законодательства, международных нормативно-</p> | <p>Коллоквиум</p> | <p>Зачёт: Контрольные вопросы</p> |

| | | | | |
|---------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|
| | | <p>правовых актов и судебной практики применительно к конкретной ситуации</p> <p>ПК МП-5.2: <i>Знать:</i> порядок обращения, требования к заявителям, содержание жалобы в международные судебные органы; порядок и особенности применения международных нормативно-правовых актов и судебной практики для решения конкретной ситуации <i>Уметь:</i> готовить документы, необходимые для обращения в суд по различным категориям дел <i>Владеть:</i> навыками составления текста юридических документов для обращения в судебные инстанции; достаточными владения иностранными языками (английский, французский) для участия в международном судебном процессе</p> <p>ПК МП-5.3: <i>Знать:</i> порядок и особенности устного этапа разбирательства в международных судах; процессуальные процедуры конкретного международного суда <i>Уметь:</i> готовить устное выступление в суде, устно защищать подготовленную позицию <i>Владеть:</i> достаточными навыками общения на иностранном языке (английский, французский) для участия в международном судебном процессе; навыками представления доверителя в устном разбирательстве</p> | | |
| ПК МП-6: Способен участвовать в | ПК МП-6.1: Составляет жалобы и иные | ПК МП-6.1: <i>Знать:</i> правила составления | Контрольная работа | Зачёт: |

| | | | | |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|
| <p>обеспечении национального и международного судопроизводства.</p> | <p>процессуальные документы, применяя знания международно-правовых норм и отечественного права ПК МП-6.2: Представляет в суд процессуальные документы в соответствии с правилами, предусмотренными международно-правовыми нормами и нормами российского законодательства ПК МП-6.3: Знает международное и российское законодательство и правоприменительную практику об исполнительном производстве</p> | <p>процессуальных документов Уметь: правильно составлять и оформлять процессуальные документы Владеть: способностью составить и подготовить процессуальные документы ПК МП-6.2: Знать: понятие и классификацию доказательств, правила относимости, допустимости, достоверности и достаточности доказательств Уметь: применять знания о доказательствах на практике Владеть: навыками сбора и предоставления доказательств ПК МП-6.3: Знать: основных положений отраслевых юридических и специальных наук, сущности и содержания основных понятий, категорий, институтов процессуального законодательства Уметь: анализировать, толковать и правильно применять процессуальные нормы Владеть: навыками анализа и обобщения практики применения норм процессуального законодательства</p> | <p>Эссе</p> | <p>Проект</p> |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

| | |
|------------------------------------------------|--------------|
| | очная |
| Общая трудоемкость, з.е. | 2 |
| Часов по учебному плану | 72 |
| в том числе | |
| аудиторные занятия (контактная работа): | |

| | |
|--------------------------------------------------------------------------|------------|
| - занятия лекционного типа | 16 |
| - занятия семинарского типа (практические занятия / лабораторные работы) | 16 |
| - КСР | 1 |
| самостоятельная работа | 39 |
| Промежуточная аттестация | 0 Зачёт |

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

| Наименование разделов и тем дисциплины | Всего (часы) | в том числе | | | Самостоятельная работа обучающегося, часы |
|-------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------|-------------------------------------------|
| | | Контактная работа (работа во взаимодействии с преподавателем), часы из них | | | |
| | | Занятия лекционного типа | Занятия семинарского типа (практические занятия/лабораторные работы), часы | Всего | |
| Ф Ф Ф | Ф Ф Ф | Ф Ф Ф | Ф Ф Ф | Ф Ф Ф | |
| Тема 1. Международное информационное право, как комплексная отрасль современного международного права | 8 | 2 | 2 | 4 | 4 |
| Тема 2. Содержание категории «информационная безопасность» | 6 | 1 | 1 | 2 | 4 |
| Тема 3. Международные нормы и стандарты в области информационной безопасности | 8 | 2 | 2 | 4 | 4 |
| Тема 4. Международные средства защиты свободы слова и самовыражения | 8 | 2 | 2 | 4 | 4 |
| Тема 5. Правовые гарантии информационной безопасности государства | 9 | 2 | 2 | 4 | 5 |
| Тема 6. Право информационной войны | 8 | 2 | 2 | 4 | 4 |
| Тема 7. Борьба с информационной преступностью | 9 | 2 | 2 | 4 | 5 |
| Тема 8. Информационная безопасность в практике международных отношений | 7 | 1 | 1 | 2 | 5 |
| Тема 9. Влияние инноваций на внутреннюю и международную информационную безопасность | 8 | 2 | 2 | 4 | 4 |
| Аттестация | 0 | | | | |
| КСР | 1 | | | 1 | |
| Итого | 72 | 16 | 16 | 33 | 39 |

Содержание разделов и тем дисциплины

Тема 1. Международное информационное право, как комплексная отрасль современного международного права

1. Понятие и предмет международного информационного права. Определение информации в международном праве
2. Принципы международного информационного права. Базовые принципы информационной безопасности.
3. Понятие и теоретические концепции информационного общества

4. Правосубъектность в международном информационном праве. Государства, как основные субъекты разработки и реализации норм информационного права
5. Основные проблемы и конфликты в сфере международного информационного права
6. Развитие международного информационного права в свете современных технологий

Тема 2. Содержание категории «информационная безопасность»

1. Соотношение понятий «информационная безопасность» и «кибербезопасность»
2. Основные цели и задачи информационной безопасности
3. Угрозы международной информационной безопасности
4. Объекты информационной безопасности
5. Субъекты информационного воздействия – государства и негосударственные акторы
6. Новые технологии и их влияние на информационную безопасность
7. Формирование концепции информационного суверенитета государства.

Тема 3. Международные нормы и стандарты в области информационной безопасности

1. Международные организации, играющие ключевую роль в разработке норм и стандартов информационной безопасности
2. Основные международные стандарты в области информационной безопасности
3. Основные международные соглашения и конвенции, касающиеся информационной безопасности
4. Различия в подходах к информационной безопасности в разных регионах мира. Взаимодействие универсальных и региональных стандартов
5. Влияние международных стандартов на практику обеспечения информационной безопасности
6. Последствия несоблюдения международных норм и стандартов в области информационной безопасности

Тема 4. Международные средства защиты свободы слова и самовыражения

1. Международно-правовые гарантии свободы слова и самовыражения
2. Ограничения свободы слова в международном информационном праве
3. Запрещенная и ограниченная к распространению информация: международные и национальные нормы
4. Соотношение защиты интересов государства с информационными правами и свободами частных лиц: анализ ситуации в России и иностранных государствах
5. Неправительственные организации, принимающие участие в механизме защиты свободы слова и самовыражения
6. Национальные подходы к регулированию социальных сетей

Тема 5. Правовые гарантии информационной безопасности государства

1. Международные гарантии информационной безопасности государства
2. Содержание и основные направления информационного противоборства государств в современных международных отношениях
3. Информационные средства воздействия: понятие, виды
4. Защита информации в системе безопасности государства. Понятие критической информационной инфраструктуры государства
5. Объекты и субъекты критической информационной инфраструктуры
6. Роль СНГ и ОДКБ в обеспечении безопасности критической информационной инфраструктуры государств-участниц

Тема 6. Право информационной войны

1. Информационная война как средство достижения политических целей. Интересы в информационной области

2. Информационное оружие: понятие и виды, реальные последствия информационного воздействия. Информационное оружие – оружие массового поражения
3. Угрозы международной информационной безопасности как вызов современной стратегической стабильности
4. Международное право вооруженных конфликтов и его применимость к действиям в информационной сфере. Таллинское руководство по международному праву, применимому к кибернетическим войнам и «Таллин 2.0»
5. Применимость международного права в области разоружения к вопросу ограничения информационного оружия
6. Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства

Тема 7. Борьба с информационной преступностью

1. Понятие "кибератаки" в международном праве, критерии, используемые для классификации кибератак
2. Криминальные угрозы международной информационной безопасности
3. Использование Интернета организованными преступными группами и сообществами
4. Проблемы противодействия использованию в преступной деятельности средств обеспечения анонимности пользователей Интернета
5. Информационный (кибер-) терроризм
6. Криминализация киберпреступлений в практике государств
7. Роль международных организаций (Интерпол, Европол, ...) в борьбе с информационной преступностью

Тема 8. Информационная безопасность в практике международных отношений

1. Международное сотрудничество в сфере международной информационной безопасности
2. Деятельность ООН в развитии международно-правового регулирования информационных отношений: «Глобальный цифровой договор» 2024 года, декларации Генеральной Ассамблеи о трансформации общества в цифровую эпоху
3. Российские инициативы в области международной информационной безопасности
4. Иностранная практика правового обеспечения информационной безопасности (на примере США, КНР, КНДР, стран Евросоюза и т.д.)
5. Обеспечение информационной безопасности Российской Федерации в аспекте глобальных политических процессов современного мира

Тема 9. Влияние инноваций на внутреннюю и международную информационную безопасность

1. Искусственный интеллект: понятие, типы и сфера применения
2. Международные и этические стандарты в области регулирования ИИ
3. Сценарии позитивного и негативного влияния ИИ на информационную безопасность
4. Смертоносные автономные системы вооружений: правовое регулирование «роботов-убийц»
5. Как инновации в области анализа данных могут помочь в выявлении и предотвращении внутренних угроз безопасности
6. Инновации в области управления идентификацией и доступом (IAM), улучшение защиты корпоративных данных
7. Влияние дезинформации на внутреннюю и международную политику

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:

Электронные курсы, созданные в системе электронного обучения ННГУ:

Международное и внутригосударственное регулирование информационной безопасности, <https://e-learning.unn.ru/course/view.php?id=2969>.

Иные учебно-методические материалы:

Для успешного усвоения курса необходимо не только посещать аудиторные занятия, но и вести активную самостоятельную работу. При самостоятельной проработке курса обучающиеся должны:

- просматривать основные определения и факты;
- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- изучить рекомендованную основную и дополнительную литературу, составлять тезисы, аннотации и конспекты наиболее важных аспектов;
- самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
- использовать для самопроверки материалы фонда оценочных средств;
- выполнять домашние задания по указанию преподавателя.

Самостоятельная работа обучающегося направлена на решение следующих задач:

- 1) закрепление владения юридическими понятиями и категориями;
- 2) анализ юридических фактов и возникающих в связи с ними правовых отношений, характеризующих специфику становления права международной и европейской безопасности;
- 3) анализ политико-правовых процессов и факторов, сопоставления российской и зарубежных доктрин национальной, европейской и международной информационной безопасности;
- 4) развитие логического мышления, развитие навыков создания научных работ, ведения научных дискуссий.

Для решения указанных задач студентам предлагаются к прочтению и содержательному анализу нормативные тексты, являющиеся правовой базой, определяющей состояние развития современного международного права, а также научные труды, формирующие основу права международной информационной безопасности.

Студенты выполняют задания самостоятельно, обращаясь к учебной, справочной и научной литературе. Проверка выполнения заданий осуществляется с помощью письменных самостоятельных (контрольных) работ и тестов.

Результаты выполнения домашнего задания оцениваются по следующим критериям:

- 1) степень и уровень выполнения задания;
- 2) использование специальной литературы, монографий и научных трудов;
- 3) логика изложения материала;
- 4) наличие элементов сравнительного анализа, его уместность и обоснованность;
- 5) самостоятельность суждений и выводов;
- 6) наличие аргументации и ее убедительность;

7) аккуратность в оформлении работы;

8) сдача домашнего задания в срок.

Баллы за результаты выполнения домашнего задания влияют на оценку по текущей успеваемости.

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Кейс-задача) для оценки сформированности компетенции УК-5:

Задачи, решение которых следует прокомментировать, продемонстрировав уровень знания нормативного материала и теоретических основ международного и национального права и права международной информационной безопасности.

Задача 1.

Фабула: Государство А обвиняет Государство Б в проведении масштабной кибератаки на свою критическую инфраструктуру, включая энергетические сети, банковскую систему и правительственные порталы. В результате атаки произошли массовые отключения электроэнергии, сбои в работе финансовых учреждений и утечка конфиденциальных данных государственных служащих. Государство А утверждает, что атака была совершена хакерской группой, которая, по данным разведки, связана с правительственными структурами Государства Б.

Государство Б отрицает свою причастность к атаке, заявляя, что хакерская группа действовала независимо, и обвиняет Государство А в использовании инцидента для политического давления. В ответ Государство Б вводит санкции против Государства А, ограничивая доступ к своим цифровым платформам и сервисам.

Вопросы для анализа:

- 1) *Какие нормы международного права могут быть применены для разрешения данного конфликта?*
- 2) *Какую роль играют Будапештская конвенция о киберпреступности и Таллинское руководство 2.0 в данной ситуации?*
- 3) *Как можно доказать связь между хакерской группой и государственными структурами?*
- 4) *Какие меры может предпринять Государство А в рамках международного права для защиты своих интересов?*
- 5) *Являются ли санкции, введённые Государством Б, правомерными с точки зрения международного права?*

Задача 2.

Фабула: Группа хакеров, называющая себя "Свободная коалиция хакеров", провела серию кибератак на объекты ядерной инфраструктуры в нескольких странах. Хакеры заявили, что их целью было привлечение внимания к уязвимостям в системах безопасности ядерных объектов, которые могут быть использованы злоумышленниками с более опасными намерениями.

Хакеры получили удалённый доступ к системам управления ядерными объектами и изменили режимы их эксплуатации, но при этом не причинили физического ущерба объектам и не нарушили их работу. После атак группа опубликовала в "Одноклассниках" подробный отчёт о проведённых операциях, включая технические детали уязвимостей, а также призвала правительства и компании усилить кибербезопасность критической инфраструктуры.

Вопросы для анализа:

- 1) *Считается ли данный инцидент киберпреступлением? Если да, то к какому виду киберпреступности он относится?*
- 2) *Можно ли рассматривать действия хакеров как форму кибертерроризма или кибершпионажа?*
- 3) *Есть ли основания считать действия хакеров "этичным взломом" (ethical hacking), если их целью было улучшение безопасности?*
- 4) *Какие нормы международного права могут быть применены к данному случаю?*
- 5) *Какую роль играет концепция "критической инфраструктуры" в международном праве и как она регулируется?*
- 6) *Кто несёт ответственность за инцидент: хакеры, компании, управляющие ядерными объектами, или государственные органы, отвечающие за безопасность?*
- 7) *Какие меры могут быть приняты против платформы "Одноклассники", если она не удалила публикации хакеров, содержащие технические детали уязвимостей?*
- 8) *Какие уязвимости в системах безопасности ядерной инфраструктуры могли быть использованы хакерами?*

Задача 3.

Фабула: Международная группа мошенников создала фейковую криптовалюту под названием "LobachCoin". Они провели масштабную рекламную кампанию, убеждая инвесторов по всему миру вкладывать средства в эту "инновационную и безопасную" криптовалюту. Мошенники утверждали, что LobachCoin поддерживается ведущими технологическими компаниями и правительствами нескольких стран, хотя на самом деле это было ложью.

Через несколько месяцев после запуска LobachCoin мошенники провели "exit scam" (схему выхода): они заблокировали доступ инвесторов к их кошелькам и исчезли с более чем \$1 млрд в различных криптовалютах. Пострадали тысячи инвесторов из разных стран, включая частных лиц, компании и даже государственные фонды.

Вопросы для анализа:

- 1) Какие виды киберпреступлений можно выделить в данном случае?
- 2) Можно ли квалифицировать действия мошенников как кибертерроризм?
- 3) Какие международные соглашения и конвенции могут быть применены для расследования и преследования мошенников?
- 4) Какую роль могут играть Интерпол, Европол и другие международные организации в расследовании этого дела?
- 5) Какие юрисдикционные проблемы могут возникнуть, если мошенники находятся в одной стране, а их серверы и жертвы — в других?
- 6) Какую роль могут играть национальные регуляторы в регулировании криптовалютных проектов?
- 7) Какие риски возникают для глобальной финансовой системы из-за распространения криптовалютных мошенничеств?

Критерии оценивания (оценочное средство - Кейс-задача)

| Оценка | Критерии оценивания |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| превосходно | Знание нормативной базы и доктрины международного права выше уровня, предусмотренного программой, свободное владение терминологическим аппаратом, системность знаний, способность к анализу специфики действия норм международного права |
| отлично | Задание выполнено полностью; решение обосновано логично и последовательно, с точными и соответствующими ссылками на первоисточник |
| очень хорошо | Задание выполнено с незначительными погрешностями, допущены неточности в ссылках на нормативные акты |
| хорошо | Задание выполнено с незначительными погрешностями, допущены неточности в решении |
| удовлетворительно | Демонстрирует знания и понимание большей части задания, но решение казуса не завершено логически, отсутствуют ссылки на статьи нормативного акта |
| неудовлетворительно | Задание решено неверно, проявлен недостаточный уровень знаний и умений, студент не способен пояснить полученный результат |
| плохо | Задание не выполнено |

5.1.2 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции УК-5:

1. Что понимается под информационной безопасностью:

- а) защита душевного здоровья телезрителей
- б) защита от нанесения неприемлемого ущерба субъектам информационных отношений
- в) обеспечение информационной независимости России

2. Сложность обеспечения информационной безопасности является следствием:

- а) невнимания широкой общественности к данной проблематике
- б) все большей зависимости общества от информационных систем
- в) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

3. Что из перечисленного относится к числу основных аспектов информационной безопасности:

- а) подотчетность - полнота регистрационной информации о действиях субъектов
- б) приватность - сокрытие информации о личности пользователя
- в) конфиденциальность - защита от несанкционированного ознакомления

4. На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют:

- а) меры ограничительной направленности
- б) направляющие и координирующие меры
- в) меры по обеспечению информационной независимости

5. Меры информационной безопасности направлены на защиту от:

- а) нанесения неприемлемого ущерба
- б) нанесения любого ущерба
- в) подглядывания в замочную скважину

6. Уголовный кодекс РФ не предусматривает наказания за:

- а) неправомерный доступ к компьютерной информации
- б) создание, использование и распространение вредоносных программ
- в) массовую рассылку незапрошенной рекламной информации

7. Уровень безопасности С, согласно «Оранжевой книге», характеризуется:

- а) произвольным управлением доступом
- б) принудительным управлением доступом
- в) верифицируемой безопасностью

Критерии оценивания (оценочное средство - Тест)

| Оценка | Критерии оценивания |
|------------|-------------------------------|
| зачтено | 51-100% правильных ответов |
| не зачтено | менее 51 % правильных ответов |

5.1.3 Типовые задания (оценочное средство - Коллоквиум) для оценки сформированности компетенции ПК МП-5:

1. Международное информационное право, как комплексная отрасль современного международного права.
2. Становление права информационной безопасности.
3. Содержание категории «информационная безопасность».
4. Правосубъектность в международном информационном праве.
5. Свобода информации в международном праве. Международные средства защиты свободы слова и самовыражения.
6. Правовые гарантии информационной безопасности государства и систем международной связи.
7. Право информационной войны.
8. Информационная безопасность в практике международных отношений.

Критерии оценивания (оценочное средство - Коллоквиум)

| Оценка | Критерии оценивания |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| превосходно | Самостоятельное и оригинальное осмысление материала; ясное и убедительное рассуждение; мощный и убедительный анализ, указаны нормы международных соглашений, приведены примеры из международной судебной практики |
| отлично | Четкость логики и анализа, оригинальность в осмыслении материала, в целом работа хорошо аргументирована и убедительна, указаны нормы международных соглашений, приведены примеры из международной |

| Оценка | Критерии оценивания |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | судебной практики |
| очень хорошо | Четкость логики и анализа, оригинальность в осмыслении материала, в целом работа хорошо аргументирована и убедительна, указаны нормы международных соглашений |
| хорошо | Четкость логики и анализа, некоторая оригинальность в осмыслении материала, в целом работа хорошо аргументирована и убедительна |
| удовлетворительно | Удовлетворительное построение и анализ при отсутствии оригинальности или критического осмысления материала |
| неудовлетворительно | Логика слабая, оригинальность отсутствует и/или материал недостаточно критически осмыслен |
| плохо | Логика крайне слабая, отсутствует или неадекватна выбранной теме |

5.1.4 Типовые задания (оценочное средство - Контрольная работа) для оценки сформированности компетенции ПК МП-6:

Вопросы для контроля:

1. Понятие «информации» в международном праве.
2. Информационное общество. Идея информационного общества. Теоретические концепции информационного общества. Политические риски.
3. Принципы международного информационного права. Базовые принципы информационной безопасности.
4. Особенности создания и реализации МП обычных и договорных норм в сфере управления интернетом.
5. Информатизация и глобализации.
6. Международные информационные правовые отношения.
7. Международный информационный правопорядок.
8. Международный опыт правового обеспечения информационной безопасности.
9. Международно-правовые аспекты использования информационно-коммуникационных технологий
10. Адаптация права международной безопасности к использованию ИКТ.

11. Трансформация концепции государственного суверенитета в условиях глобального информационного общества.
12. Основные направления информационного противоборства.
13. Объекты информационной безопасности. Безопасность открытых информационных сетей. Информационная безопасность бизнеса. Информационно-психологическая безопасность.
14. Угрозы международной информационной безопасности. Принципы классификации и источники угроз информационной безопасности.
15. Субъекты информационного воздействия.
16. Массовые коммуникации и международное право.
17. Средства массовой информации и международная правосубъектность.
18. Статус индивида в международном информационном праве.
19. Неправительственные организации в сфере массовых коммуникаций, международной журналистики, связей с общественностью и рекламы.
20. Идея свободы информации и ее реализация.
21. Международно-правовые гарантии свободы самовыражения.
22. Свобода слова и условия её реализации.
23. Международная практика защиты свободы слова и самовыражения.
24. Международные гарантии информационной безопасности государства.
25. Информационное противоборство и международные отношения.
26. Защита информации и информационная безопасность государства.
27. Международное сообщество, коммуникации и культурный обмен.
28. Правовые аспекты сотрудничества государств в сфере массовых коммуникаций.
29. Правовой режим сетей связи общего пользования.
30. Информационное оружие – новый вид оружия массового поражения.
31. Информационный (кибер-) терроризм.
32. Интересы в информационной области.
33. Международное право вооруженных конфликтов и его применимость к действиям в информационной сфере.

34. Применимость международного права в области разоружения к вопросу ограничения информационного оружия.
35. Применение МГП к вооруженным конфликтам в киберпространстве. Адаптация международного права к конфликтам в киберпространстве.
36. Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства.
37. Российские инициативы по международной информационной безопасности.
38. Переговорный процесс и международное сотрудничество в области ограничения информационных видов оружия.
39. Перспективы установления международного контроля над информационными видами вооружений.

Критерии оценивания (оценочное средство - Контрольная работа)

| Оценка | Критерии оценивания |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| превосходно | Знание нормативной базы и доктрины международного права выше уровня, предусмотренного программой, свободное владение терминологическим аппаратом, системность знаний, способность к анализу специфики действия норм международного права |
| отлично | Задание выполнено полностью; решение обосновано логично и последовательно, с точными и соответствующими ссылками на первоисточник |
| очень хорошо | Задание выполнено с незначительными погрешностями, допущены неточности в ссылках на нормативные акты |
| хорошо | Задание выполнено с незначительными погрешностями, допущены неточности в решении |
| удовлетворительно | Демонстрирует знания и понимание большей части задания, но решение казуса не завершено логически, отсутствуют ссылки на статьи нормативного акта |
| неудовлетворительно | Задание решено неверно, проявлен недостаточный уровень знаний и умений, студент не способен пояснить полученный результат |
| плохо | Задание не выполнено |

5.1.5 Типовые задания (оценочное средство - Эссе) для оценки сформированности компетенции ПК МП-6:

1. Международный опыт правового обеспечения информационной безопасности.

2. Массовые коммуникации и международное право.
3. Статус индивида в международном информационном праве.
4. Неправительственные организации в сфере массовых коммуникаций.
5. Международные средства защиты свободы слова и самовыражения.
6. Международные гарантии информационной безопасности.
7. Информационное противоборство и международные отношения.
8. Защита информации и информационная безопасность.
9. Правовые аспекты сотрудничества государств в сфере массовых коммуникаций.
10. Правовой режим сетей связи общего пользования.
11. Правовое положение субъектов международной журналистики.
12. Правовые аспекты деятельности журналистов в зоне вооруженных конфликтов.
13. Международно-правовые стандарты безопасности рекламы.
14. Международная реклама и защита национальных интересов государств.
15. Международные гарантии безопасности политической рекламы.
16. Правовая охрана произведений и интересы безопасности государств.
17. Международно-правовые гарантии защиты авторских прав.
18. Международное право вооруженных конфликтов и его применимость к действиям в информационной сфере.
19. Применимость международного права в области разоружения к вопросу ограничения информационного оружия.

Критерии оценивания (оценочное средство - Эссе)

| Оценка | Критерии оценивания |
|------------|------------------------------------------------------------------------------------------------------------------|
| зачтено | Тема раскрыта полностью, логично и последовательно; работа выполнена самостоятельно, без неэтичных заимствований |
| не зачтено | Тема не раскрыта, либо раскрыта не полностью; Есть неэтичные заимствования, низкая степень самостоятельности |

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

| Уровень сформированности компетенций (индикатора достижения компетенций) | плохо | неудовлетворительно | удовлетворительно | хорошо | очень хорошо | отлично | превосходно |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| | не зачтено | | | зачтено | | | |
| <u>Знания</u> | Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа | Уровень знаний ниже минимальных требований. Имели место грубые ошибки | Минимально допустимый уровень знаний. Допущено много негрубых ошибок | Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок | Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок | Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет. | Уровень знаний в объеме, превышающем программу подготовки. |
| <u>Умения</u> | Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа | При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки | Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме | Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами | Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами | Продемонстрированы все основные умения. Решены все основные задачи с отдельным и несущественными недочетами, выполнены все задания в полном объеме | Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов |
| <u>Навыки</u> | Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа | При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки | Имеется минимальный набор навыков для решения стандартных задач с некоторым и недочетами | Продемонстрированы базовые навыки при решении стандартных задач с некоторым и недочетами | Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов | Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов | Продемонстрирован творческий подход к решению нестандартных задач |

Шкала оценивания при промежуточной аттестации

| Оценка | Уровень подготовки |
|--------|--------------------|
|--------|--------------------|

| | | |
|-------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | |
| зачтено | превосходно | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой |
| | отлично | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично». |
| | очень хорошо | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо» |
| | хорошо | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо». |
| | удовлетворительно | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно» |
| не зачтено | неудовлетворительно | Хотя бы одна компетенция сформирована на уровне «неудовлетворительно». |
| | плохо | Хотя бы одна компетенция сформирована на уровне «плохо» |

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции УК-5

1. Понятие и предмет международного информационного права. Определение информации в международном праве.
2. Принципы международного информационного права. Базовые принципы информационной безопасности.
3. Понятие и теоретические концепции информационного общества.
4. Правосубъектность в международном информационном праве. Государства, как основные субъекты разработки и реализации норм информационного права.
5. Основные проблемы и конфликты в сфере международного информационного права.
6. Развитие международного информационного права в свете современных технологий.
7. Соотношение понятий «информационная безопасность» и «кибербезопасность».
8. Основные цели и задачи информационной безопасности.
9. Угрозы международной информационной безопасности.
10. Объекты информационной безопасности.
11. Субъекты информационного воздействия – государства и негосударственные акторы.
12. Новые технологии и их влияние на информационную безопасность.
13. Формирование концепции информационного суверенитета государства.
14. Международные организации, играющие ключевую роль в разработке норм и стандартов информационной безопасности.
15. Основные международные стандарты в области информационной безопасности.
16. Основные международные соглашения и конвенции, касающиеся информационной безопасности.

17. Различия в подходах к информационной безопасности в разных регионах мира. Взаимодействие универсальных и региональных стандартов.
18. Влияние международных стандартов на практику обеспечения информационной безопасности.
19. Последствия несоблюдения международных норм и стандартов в области информационной безопасности.
20. Международно-правовые гарантии свободы слова и самовыражения.
21. Ограничения свободы слова в международном информационном праве.
22. Запрещенная и ограниченная к распространению информация: международные и национальные нормы.
23. Соотношение защиты интересов государства с информационными правами и свободами частных лиц; анализ ситуации в России и иностранных государствах.
24. Неправительственные организации, принимающие участие в механизме защиты свободы слова и самовыражения.
25. Национальные подходы к регулированию социальных сетей.
26. Международные гарантии информационной безопасности государства.
27. Содержание и основные направления информационного противоборства государств в современных международных отношениях.
28. Информационные средства воздействия: понятие, виды.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК МП-5

1. Защита информации в системе безопасности государства. Понятие критической информационной инфраструктуры государства.
2. Объекты и субъекты критической информационной инфраструктуры.
3. Роль СНГ и ОДКБ в обеспечении безопасности критической информационной инфраструктуры государств-участниц.
4. Информационная война как средство достижения политических целей. Интересы в информационной области.
5. Информационное оружие: понятие и виды, реальные последствия информационного воздействия. Информационное оружие – оружие массового поражения.
6. Угрозы международной информационной безопасности как вызов современной стратегической стабильности.
7. Международное право вооруженных конфликтов и его применимость к действиям в информационной сфере. Таллинское руководство по международному праву, применимому к кибернетическим войнам и «Таллин 2.0».
8. Применимость международного права в области разоружения к вопросу ограничения информационного оружия.
9. Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства.
10. Понятие "кибератаки" в международном праве, критерии, используемые для классификации кибератак.
11. Криминальные угрозы международной информационной безопасности.
12. Использование Интернета организованными преступными группами и сообществами.
13. Проблемы противодействия использованию в преступной деятельности средств обеспечения анонимности пользователей Интернета.
14. Информационный (кибер-) терроризм.
15. Криминализация киберпреступлений в практике государств.
16. Роль международных организаций (Интерпол, Европол, ...) в борьбе с информационной преступностью.
17. Международное сотрудничество в сфере международной информационной безопасности.

18. Деятельность ООН в развитии международно-правового регулирования информационных отношений: «Глобальный цифровой договор» 2024 года, декларации Генеральной Ассамблеи о трансформации общества в цифровую эпоху.
19. Российские инициативы в области международной информационной безопасности.
20. Иностранная практика правового обеспечения информационной безопасности (на примере США, КНР, КНДР, стран Евросоюза и т.д.).
21. Обеспечение информационной безопасности Российской Федерации в аспекте глобальных политических процессов современного мира.
22. Искусственный интеллект: понятие, типы и сфера применения.
23. Международные и этические стандарты в области регулирования ИИ.
24. Сценарии позитивного и негативного влияния ИИ на информационную безопасность.
25. Смертоносные автономные системы вооружений: правовое регулирование «роботов-убийц».
26. Как инновации в области анализа данных могут помочь в выявлении и предотвращении внутренних угроз безопасности.
27. Инновации в области управления идентификацией и доступом (IAM), улучшение защиты корпоративных данных.
28. Влияние дезинформации на внутреннюю и международную политику.

Критерии оценивания (оценочное средство - Контрольные вопросы)

| Оценка | Критерии оценивания |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| зачтено | Компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне от «удовлетворительно» до «превосходно» |
| не зачтено | Компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне «неудовлетворительно» или «плохо» |

5.3.3 Типовые задания (оценочное средство - Проект) для оценки сформированности компетенции ПК МП-6

Индивидуально или в группе (до 2 участников) подготовьте проект по одной из предложенных тем. Проект предполагает самостоятельное исследование актуальной проблемы или ситуации международной безопасности с оформлением его результатов в форме презентации Power Point с публичной защитой.

1. Какие меры на уровне международного права следовало бы предпринять для повышения уровня международной кибер-безопасности? Сформулируйте свои предложения.
2. Является ли ограничение доступа в Интернет нарушением фундаментальных прав человека?
3. Информационное оружие и его использование в вооруженных конфликтах
4. Даркнет как площадка для совершения преступлений
5. Безопасность и перспективы электронного государства

Критерии оценивания (оценочное средство - Проект)

| Оценка | Критерии оценивания |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------|
| зачтено | Задание выполнено полностью; решение обосновано логично и последовательно, с точными и соответствующими ссылками на нормы международного права |

| Оценка | Критерии оценивания |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| не зачтено | Задание не выполнено либо решено не верно, проявлен недостаточный уровень знаний и умений, студент не способен пояснить полученный результат |

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Архипов В. В. Интернет-право : учебник и практикум / В. В. Архипов. - Москва : Юрайт, 2023. - 249 с. - (Высшее образование). - ISBN 978-5-534-03343-4. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=844091&idb=0>.
2. Бачило И. Л. Информационное право : учебник / И. Л. Бачило. - 5-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 419 с. - (Высшее образование). - ISBN 978-5-534-00608-7. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=845310&idb=0>.
3. Рассолов И. М. Информационное право : учебник и практикум / И. М. Рассолов. - 6-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 415 с. - (Высшее образование). - ISBN 978-5-534-14327-0. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=846432&idb=0>.

Дополнительная литература:

1. Абашидзе Аслан Хусейнович. Международное право : Учебник / Российский университет дружбы народов; Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя; Тюменский государственный университет; Дипломатическая академия Министерства иностранных дел Российской Федерации. - 4-е изд. ; перераб. - Москва : ООО "Юридическое издательство Норма", 2018. - 576 с. - ВО - Бакалавриат. - ISBN 978-5-91768-469-7. - ISBN 978-5-16-100858-4. - ISBN 978-5-16-009597-4., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=741784&idb=0>.
2. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. - Москва : Юрайт, 2023. - 325 с. - (Профессиональное образование). - ISBN 978-5-534-00843-2. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=843572&idb=0>.
3. Крутских А.В. Инновационные направления современных международных отношений : учебное пособие / Крутских А.В.; Бирюков А.В. - Москва : Аспект-Пресс, 2010. - 295 с. - ISBN 978-5-7567-0562-1., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=772439&idb=0>.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

1. Электронно-библиотечная система biblio-online.ru
2. Электронно-библиотечная система Издательства «Лань» - e.lanbook.com
3. Электронно-библиотечная система znanium.com
4. Электронная коллекция книг «MyLibrary» - <http://lib.mylibrary.com/>
5. Система электронного обучения ННГУ - <https://e-learning.unn.ru/>

6. Электронный курс «Международное и внутригосударственное регулирование информационной безопасности» <https://e-learning.unn.ru/course/view.php?id=2969>
7. СПС «Консультант плюс»
8. СПС «Гарант»
9. <http://www.un.org> – сайт ООН
10. <http://www.un.org/russian/> – сайт ООН на русском языке
11. <http://www.ohchr.org/> – сайт Управления Верховного комиссара ООН по правам человека
12. <http://www.mid.ru> – официальный сайт Министерства иностранных дел России.
13. <http://www.kremlin.ru> – официальная интернет-страница Президента Российской Федерации.
14. <http://www.coe.int> – сайт Совета Европы
15. <https://www.coe.int/ru/web/commissioner/home> – сайт Комиссара Совета Европы по правам человека
16. <http://cis.minsk.by/> – официальный сайт Исполнительного комитета Содружества Независимых Государств.
17. <https://pace.coe.int/en/> – страница Парламентской Ассамблеи Совета Европы
18. <https://www.coe.int/en/web/cybercrime/home> - сайт Будапештской конвенции о киберпреступности
19. www.osce.org – официальный сайт Организации по безопасности и сотрудничеству в Европе
20. namib.online – Национальная Ассоциация международной информационной безопасности (НАМИБ)
21. <http://www.echr.coe.int> – сайт Европейского Суда по правам человека
22. en.unesco.org – официальный сайт ЮНЕСКО
23. <http://www.law.unn.ru/ceeals/> - Центр европейских и евразийских правовых исследований (ЦЕЕАПИ)

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 40.03.01 - Юриспруденция.

Автор(ы): Споршев Александр Михайлович.

Заведующий кафедрой: Орлова Юлия Михайловна, кандидат юридических наук.

Программа одобрена на заседании методической комиссии от 25.11.2024, протокол № 5.