Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Брикс кафедра»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №15 от 18 марта 2025 г.

Рабочая программа дисциплины

«МЕЖДУНАРОДНОЕ ПРАВО ПО КИБЕРЗАЩИТЕ / INTERNATIONAL LAW ON CYBER SECURITY»

Направление: 09.03.01 Информатика и вычислительная техника

Искусственный интеллект и компьютерные науки /Artificial Intelligence and Computer Science

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Усов Евгений Геннадьевич Дата подписания: 18.06.2025	Документ подписан простой электронной подписью Утвердил: Киреенко Анна Павловна Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Согласовал: Афанасьев Александр Диомидович Дата подписания: 18.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Международное право по киберзащите / International Law on Cyber Security» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ДК-1 Способность осуществлять деятельность, находящуюся за пределами непосредственной профессиональной сферы	ДК-1.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ДК-1.1	Осуществляет профессиональную деятельность в соответствии с международным правом по киберзащите	**Знать** Основные источники международного права в сфере кибербезопасности (резолюции ООН, Будапештская конвенция, нормы международного гуманитарного права). Принципы государственного суверенитета и невмешательства в киберпространстве. Международные организации, регулирующие вопросы кибербезопасности (ООН, НАТО, ОБСЕ, ЕС, ШОС). Классификацию киберугроз в международном праве (кибершпионаж, кибертерроризм, кибервойны). Правовые механизмы привлечения к ответственности за киберпреступления на международном уровне. **Уметь** Анализировать международные правовые акты и судебную практику по киберконфликтам. Применять нормы международного права для оценки кибератак и определения их правовых последствий.

		Разрабатывать рекомендации по соблюдению международных стандартов кибербезопасности. Участвовать в моделировании правовых сценариев реагирования на киберинциденты. Сопоставлять национальное и международное законодательство в области киберзащиты. **Владеть** Навыками работы с документами ООН и других международных организаций по кибербезопасности. Методами правовой квалификации киберпреступлений в соответствии с международными нормами. Опытом применения международных правовых механизмов в профессиональной деятельности (например, взаимодействие с CERT на трансграничном уровне). Умением аргументировать позицию по вопросам киберсуверенитета и правового регулирования киберпространства. Способностью оценивать риски нарушения международного права при реализации кибероперация.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Международное право по киберзащите / International Law on Cyber Security» базируется на результатах освоения следующих дисциплин/практик: «Введение в специальность / Introduction to the specialty»

Дисциплина является предшествующей для дисциплин/практик: «Проектная деятельность / Project Development Practicum»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 6

Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	54	54
лекции	18	18
лабораторные работы	0	0
практические/семинарские занятия	36	36
Самостоятельная работа (в т.ч. курсовое проектирование)	54	54
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 6

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Основы международного права в киберпространстве	1	4			1	6	1	10	Устный опрос
2	Международные организации и кибербезопасность	2	4			2	6	1	8	Устный опрос
3	Классификация киберугроз в международном праве	3	4			3	6	1	8	Устный опрос
4	Международные конвенции и соглашения	4	2			4	6	1	8	Устный опрос
5	Киберконфликты и международное гуманитарное право	5	2			5	6	1	10	Устный опрос
6	Современные вызовы и будущее регулирования	6	2			6	6	1	10	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		18				36		54	

4.2 Краткое содержание разделов и тем занятий

Семестр № 6

№	Тема	Краткое содержание

1	Основы международного права в киберпространстве	Понятие и источники международного киберправа Принципы ООН по регулированию киберпространства Правовой статус киберпространства: дискуссии о цифровом суверенитете
2	Международные организации и кибербезопасность	Роль ООН, НАТО, ОБСЕ, ЕС и ШОС в формировании норм Кибердипломатия: механизмы международного сотрудничества Примеры резолюций (например, Группа правительственных экспертов ООН по кибербезопасности)
3	Классификация киберугроз в международном праве	Кибервойны: правовые критерии Кибертерроризм и кибершпионаж: различия и правовые последствия Ответственность государств за кибератаки (принцип due diligence)
4	Международные конвенции и соглашения	Будапештская конвенция о киберпреступности: содержание и критика Национальные и региональные инициативы (например, киберстратегии США, Китая, РФ) Проблемы экстрадиции и правовой помощи при киберпреступлениях
5	Киберконфликты и международное гуманитарное право	Применение Женевских конвенций к кибервойнам Запрещенные методы и средства в кибероперациях Защита критической инфраструктуры в военное и мирное время
6	Современные вызовы и будущее регулирования	ИИ и автономные киберсистемы: пробелы в праве Криптовалюты и Dark Web: проблемы юрисдикции Перспективы глобального договора по кибербезопасности

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 6

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Основы международного права в киберпространстве	6
2	Международные организации и кибербезопасность	6
3	Классификация киберугроз в международном праве	6
4	Международные конвенции и соглашения	6
5	Киберконфликты и международное гуманитарное право	6
6	Современные вызовы и будущее регулирования	6

4.5 Самостоятельная работа

Семестр № 6

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	54

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия; Деловая игра; Кейс-метод; Лекция с ошибками; Мозговой штурм; Тренинг; Отдельные занятия по курсу могут проводиться в форме активного практического обучения: выездных занятий с посещением организаций и мероприятий для получения новых знаний и/или повторения материала на практике. При проведении таких занятий преподаватель выступает в качестве помощника и координатора процесса, передавая активную функцию обучения студентам. Он же регулирует процесс посредством подготовки специальных заданий, проведения консультаций, оценки знаний, умений и навыков, предоставления обратной связи. Помимо получения знаний активные практические занятия развивают коммуникативные навыки, учат студентов работать в команде, решать проблемы.

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

Доклад — это устное выступление (5–7 минут) с презентацией, раскрывающее конкретный аспект темы.

Как готовиться:

Выберите актуальный аспект исследуемой темы

Соберите данные: Используйте статистику (Росстат), новости (ТАСС, РИА Новости), научные статьи.

Создайте презентацию:

Слайды должны быть лаконичными (1 идея = 1 слайд).

Добавьте графики, фото, схемы для наглядности.

Проговорите речь: Репетируйте, чтобы уложиться в время и уверенно отвечать на вопросы.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

1. Цель самостоятельной работы
Углубленное изучение международно-правовых норм, регулирующих киберпространство.

Формирование навыков анализа правовых документов, судебной практики и кейсов киберконфликтов.

Подготовка к профессиональной деятельности в сфере международной кибербезопасности.
Рекомендации по организации работы
Для теоретического блока:

Используйте официальные источники:

Сайт ООН (UNODC) – разделы по киберпреступности.

Тексты Будапештской конвенции, Таллиннского руководства.

Составляйте конспекты-схемы по структуре международных документов.

Для анализа кейсов:

Выберите реальный инцидент (например, кибератаку на энергосистему Украины в 2015 г.).

Определите:

Какой нормой международного права регулируется?

Какие государства/организации могли быть причастны?

Возможные правовые последствия.

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 6 | Устный опрос

Описание процедуры.

Устный опрос проводится с целью проверки уровня усвоения студентами теоретических знаний и их способности применять нормы международного права к конкретным

ситуациям в киберпространстве. Студент получает два вопроса: первый касается теоретических аспектов международного права в сфере кибербезопасности, второй требует анализа практического кейса или решения ситуационной задачи. На подготовку ответа отводится 15-20 минут, в течение которых разрешается пользоваться своими конспектами, но не электронными устройствами.

При ответе на теоретический вопрос студент должен продемонстрировать знание ключевых международных документов, принципов регулирования киберпространства, позиций различных государств и международных организаций по вопросам кибербезопасности. Ответ должен быть структурированным, содержать ссылки на конкретные статьи конвенций или резолюций, а также отражать понимание современных вызовов в этой области.

Практический вопрос предполагает применение полученных знаний к реальным или смоделированным ситуациям. Студенту необходимо проанализировать предложенный кейс кибератаки или международного киберконфликта, квалифицировать действия участников с точки зрения международного права, предложить возможные правовые механизмы разрешения ситуации и обосновать свою позицию.

Преподаватель может задавать дополнительные вопросы, если ответ был неполным или требует уточнения. Оценка выставляется по следующим критериям: глубина знания материала, точность использования правовых норм, логичность аргументации, умение связывать теорию с практикой. Результат объявляется сразу после завершения ответа. В случае несогласия с оценкой студент может попросить разъяснить критерии выставления отметки.

Опрос проводится в устной форме, что позволяет проверить не только знание материала, но и способность студента четко формулировать мысли, вести профессиональную дискуссию и оперативно применять правовые знания к новым ситуациям - ключевые навыки для будущей работы в сфере международной кибербезопасности.

Критерии оценивания.

оценка «отлично» выставляется студенту, если материал изложен грамотно, логически структурирован; работа содержательная и аргументированная; материал подкреплен знанием литературы и источников по теме вопроса; правильно использована юридическая терминология; присутствует четкое изложение дефиниций и классификаций, раскрытие основных признаков и характерных черт понятий, явлений, процессов; содержание работы в полной мере соответствует выбранной теме.
оценка «хорошо» выставляется при наличии незначительного нарушения логики изложения материала, допущено не более двух фактических или терминологических ошибок, присутствует неполнота или неточность в формулировках;
оценка «удовлетворительно» - существенное нарушение логики изложения материала, допущение более двух фактических или терминологических ошибок; содержание работы не в полной мере соответствует выбранной теме.
оценка «неудовлетворительно» - грубое нарушение логики изложения материала, допущение многочисленных фактических или терминологических ошибок; содержание работы не соответствует выбранной теме.

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ДК-1.1	Для "знать" – точность воспроизведения норм и принципов. Для "уметь" – корректность применения права в кейсах. Для "владеть" – глубина анализа и практическая применимость навыков.	Опрос; Дискуссия; Доклады; Тестирование.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 6, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Недифференцированный зачет по данной дисциплине проводится в форме устного собеседования с целью проверки общего уровня освоения студентами учебного материала и формирования у них профессиональных компетенций в области международно-правового регулирования кибербезопасности. Процедура предполагает подготовку студентом ответа на два вопроса билета: первый вопрос касается теоретических основ международного права в киберпространстве, второй требует анализа практической ситуации или кейса. Время на подготовку составляет 20-25 минут, в течение которых разрешается пользоваться своими конспектами лекций и семинарских занятий.

При ответе на теоретический вопрос студент должен продемонстрировать знание ключевых международных документов, принципов регулирования киберпространства, позиций различных государств и международных организаций по вопросам кибербезопасности. Ответ должен содержать ссылки на конкретные статьи конвенций, резолюций ООН, положения Таллиннского руководства и других значимых международных актов. Особое внимание уделяется пониманию студентом современных тенденций и вызовов в области международно-правового регулирования киберпространства.

Практический вопрос требует от студента умения применять полученные знания к конкретным ситуациям. Необходимо проанализировать предложенный кейс кибератаки или международного киберконфликта, квалифицировать действия участников с точки зрения международного права, предложить возможные правовые механизмы урегулирования ситуации и обосновать свою позицию. Преподаватель может задавать уточняющие вопросы, направленные на проверку глубины понимания материала.

Зачет считается пройденным, если студент продемонстрировал достаточный уровень знаний по обоим вопросам билета, смог аргументированно изложить свою позицию и

показал способность применять теоретические знания к практическим ситуациям. Результат зачета ("зачтено"/"не зачтено") объявляется сразу после завершения ответа. В случае получения оценки "не зачтено" студенту предоставляется возможность повторной сдачи в установленные учебным графиком сроки. Процедура зачета направлена на проверку не только знаний нормативного материала, но и способности студентов к профессиональной аргументации и анализу актуальных проблем международно-правового регулирования киберпространства.
Примерный перечень вопросов к зачету:
Дайте определение международного права в сфере кибербезопасности.

Назовите основные источники международного права по киберзащите.

В чем заключается принцип государственного суверенитета в киберпространстве?

Перечислите ключевые международные организации, занимающиеся вопросами кибербезопасности.

Опишите структуру и содержание Будапештской конвенции о киберпреступности.

Каковы основные положения Таллиннского руководства 2.0?

В чем заключается принцип due diligence в международном киберправе?

Дайте определение кибервойны с точки зрения международного права.

Какие виды киберпреступлений выделяются в международном праве?

Опишите правовой статус киберпространства в международном праве.

В чем заключаются основные проблемы правового регулирования киберпространства?

Назовите основные резолюции ООН по вопросам кибербезопасности.

Каковы правовые последствия кибератак для государств-участников?

Опишите механизмы международного сотрудничества в сфере кибербезопасности.

В чем заключается принцип невмешательства во внутренние дела государств в киберпространстве?

Какие существуют международные стандарты в области кибербезопасности?

Опишите роль НАТО в регулировании вопросов кибербезопасности.

Каковы правовые аспекты защиты критической инфраструктуры в международном праве?

Дайте определение кибертерроризма в международном праве.

Какие меры ответственности предусмотрены за киберпреступления в международном праве?

Опишите правовые проблемы, связанные с атрибуцией кибератак.

В чем заключаются особенности правового регулирования кибершпионажа?

Каковы правовые механизмы противодействия киберпреступности на международном уровне?

Опишите роль Интерпола в борьбе с киберпреступностью.

Каковы правовые аспекты использования кибероружия?

В чем заключаются особенности применения международного гуманитарного права в киберпространстве?

Опишите правовые проблемы, связанные с экстрадицией киберпреступников.

Каковы правовые аспекты защиты персональных данных в международном праве?

Опишите роль частного сектора в обеспечении международной кибербезопасности.

Каковы правовые проблемы, связанные с регулированием криптовалют в международном праве?

Опишите правовые аспекты деятельности хактивистских группировок.

Каковы правовые механизмы урегулирования международных киберконфликтов?

Опишите правовые проблемы, связанные с использованием искусственного интеллекта в киберпространстве.

Каковы правовые аспекты кибербезопасности в условиях вооруженных конфликтов?

Опишите роль ОБСЕ в регулировании вопросов кибербезопасности.

Каковы правовые проблемы, связанные с регулированием darknet?

Опишите правовые аспекты международного сотрудничества в области киберразведки.

Каковы правовые механизмы защиты прав человека в киберпространстве?

Опишите правовые проблемы, связанные с регулированием интернета вещей.

Каковы правовые аспекты деятельности CERT на международном уровне?

Опишите правовые проблемы, связанные с регулированием облачных технологий.

Каковы правовые аспекты защиты интеллектуальной собственности в киберпространстве?

Опишите правовые проблемы, связанные с регулированием биометрических данных.

Каковы правовые аспекты международного сотрудничества в области киберобразования?

Опишите правовые проблемы, связанные с регулированием квантовых технологий.

Каковы правовые аспекты деятельности киберподразделений вооруженных сил?

Опишите правовые проблемы, связанные с регулированием социальных сетей.

Каковы правовые аспекты международного сотрудничества в области кибермедицины?

Опишите правовые проблемы, связанные с регулированием блокчейн-технологий.

Каковы перспективы развития международного права в сфере кибербезопасности?

Пример задания:

Дайте определение кибертерроризма в международном праве.
Каковы правовые аспекты международного сотрудничества в области киберобразования?

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Ответы на уровне минимальных требований Наличие существенных пробелов Затруднения с примерами	Серьезные пробелы в знаниях Неспособность ответить на основные вопросы Многочисленные ошибки

7 Основная учебная литература

1. Аулов, В. К. Международное гуманитарное право (право вооруженных конфликтов) : Учебник для вузов / В. К. Аулов, А. Н. Сотников, Ю. Н. Туганов. – Москва : Юрайт, 2025. – 73 с. – ISBN 978-5-534-15682-9. – EDN TCOGCD.

8 Дополнительная учебная литература и справочная

1. Фирсов, Ю. И. Международное право и международные отношения / Ю. И. Фирсов. – Москва : Прометей, 2023. – 78 с. – ISBN 978-5-00172-628-9. – EDN YPPLWG.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Word

2. Свободно распространяемое программное обеспечение Power Point

12 Материально-техническое обеспечение дисциплины