МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ПРАВА

Рабочая программа дисциплины (модуля)

# МЕЖДУНАРОДНЫЙ И НАЦИОНАЛЬНЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Направление и направленность (профиль)
41.03.05 Международные отношения. Международные отношения

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Международный и национальные механизмы обеспечения кибербезопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 41.03.05 Международные отношения (утв. приказом Минобрнауки России от 15.06.2017г. №555) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

*Горян Э.В., кандидат юридических наук, договор на оказание услуг, Колледж сервиса и дизайна, Ella.Goryan@vvsu.ru*

Утверждена на заседании кафедры международных отношений и права от 11.05.2023 , протокол № 11

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Гриванов Р.И.

| ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ | |
|---|---|
| Сертификат | 1575538388 |
| Номер транзакции | 0000000000AD7C5C |
| Владелец | Гриванов Р.И. |

## 1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью освоения дисциплины «Международный и национальные механизмы обеспечения кибербезопасности» является изучение студентами стандартов в области международного и национального правового регулирования безопасности в информационной сфере.

Задачи освоения дисциплины: сформировать у студента основные знания в области регулирования кибербезопасности на международном и национальном уровнях, привить умения и навыки, необходимые для самостоятельной профессиональной деятельности

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

| Название ОПОП ВО, сокращенное | Код и формулировка компетенции | Код и формулировка индикатора достижения компетенции | Результаты обучения по дисциплине | | |
|---|---|---|---|---|---|
| | | | Код результата | Формулировка результата | |
| 41.03.05 «Международные отношения» (Б-МО) | ПКВ-1 : Способен использовать нормы и принципы международного права в качестве регуляторов международных отношений | ПКВ-1.3к : Дает оценку деятельности участников международных отношений в сфере международной безопасности и квалифицированные заключения и консультации в сфере информационной безопасности | РД1 | Знание | структуры международных и национальных механизмов обеспечения кибербезопасности |
| | | | РД1 | Умение | анализировать содержание национальных и международных стандартов обеспечения кибербезопасности |
| | | | РД1 | Навык | определения преимуществ и недостатков международного и национальных механизмов обеспечения кибербезопасности |

## 2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений, читается в 5 семестре. Усвоение студентами компетенций дисциплины контролируется фондом оценочных средств (ФОС).

## 3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Форма | | Семестр (ОФО) | Трудо-емкость | Объем контактной работы (час) | | Форма |

| Название ОПОП ВО | обучения | Часть УП | или курс (ЗФО, ОЗФО) | (З.Е.) | Всего | Аудиторная | | | Внеаудиторная | | СРС | аттестации |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | лек. | прак. | лаб. | ПА | КСР | | |
| 41.03.05 Международные отношения | ОФО | Б1.В | 5 | 2 | 37 | 18 | 18 | 0 | 1 | 0 | 35 | З |

## 4 Структура и содержание дисциплины (модуля)

### 4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

| № | Название темы | Код результата обучения | Кол-во часов, отведенное на | | | | Форма текущего контроля |
|---|---|---|---|---|---|---|---|
| | | | Лек | Практ | Лаб | СРС | |
| 1 | Информационная безопасность и кибербезопасность | РД1 | 2 | 2 | 0 | 4 | собеседование, творческое задание |
| 2 | Международный механизм обеспечения кибербезопасности | РД1, РД1, РД1 | 2 | 2 | 0 | 4 | собеседование, творческое задание |
| 3 | Национальные механизмы обеспечения кибербезопасности | РД1, РД1, РД1 | 10 | 10 | 0 | 20 | собеседование, доклад, творческое задание |
| 4 | Региональные механизмы обеспечения кибербезопасности | РД1, РД1, РД1 | 4 | 4 | 0 | 7 | собеседование, доклад, творческое задание |
| **Итого по таблице** | | | **18** | **18** | **0** | **35** | |

### 4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

*Тема 1 Информационная безопасность и кибербезопасность.*

Содержание темы: Понятие информации. Идея информационного общества. Теоретические концепции информационного общества. Информатизация и глобализация. Основные направления информационного противоборства. Новые объекты информационной безопасности. Соотношение понятий «информационная безопасность» и «кибербезопасность».

Формы и методы проведения занятий по теме, применяемые образовательные технологии: вводная лекция, практическое занятие, собеседование, творческое задание.

Виды самостоятельной подготовки студентов по теме: подготовка к собеседованию и выполнение творческого задания путем изучения основной и дополнительной литературы.

*Тема 2 Международный механизм обеспечения кибербезопасности.*

Содержание темы: Основные аспекты информационной безопасности. Информация и безопасность, информационная безопасность: определение понятий. Эволюция международно-правового регулирования информационных отношений с точки зрения обеспечения информационной безопасности. Стратегия в области информационно-коммуникационных технологий (резолюции ГА ООН). Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур (резолюции ГА ООН). Использование информационно-коммуникационных технологий в целях развития (резолюции ГА ООН). Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности (резолюции ГА ООН). Борьба с преступным

использованием информационных технологий (резолюции ГА ООН).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция-дискуссия (проблемная лекция), практическое занятие, собеседование, творческое задание.

Виды самостоятельной подготовки студентов по теме: подготовка к лекции-дискуссии (проблемной лекции), собеседованию и выполнение творческого задания путем изучения основной и дополнительной литературы.

*Тема 3 Национальные механизмы обеспечения кибербезопасности.*

Содержание темы: Национальная стратегия кибербезопасности Российской Федерации. Критическая информационная инфраструктура Российской Федерации: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Российской Федерации. Законодательство Российской Федерации в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Общие положения о государственной тайне в Российской Федерации. Перечень сведений, составляющих государственную тайну Российской Федерации. Отнесение сведений к государственной тайне и их засекречивание в Российской Федерации. Рассекречивание сведений и их носителей в Российской Федерации. Распоряжение сведениями, составляющими государственную тайну, в Российской Федерации. Защита государственной тайны в Российской Федерации. Финансирование мероприятий по защите государственной тайны в Российской Федерации. Контроль и надзор за обеспечением защиты государственной тайны в Российской Федерации. Национальная стратегия кибербезопасности Сингапура. Критическая информационная инфраструктура Сингапура: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Сингапура. Законодательство Сингапура в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности США. Критическая информационная инфраструктура США: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности США. Законодательство США в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности Великобритании. Критическая информационная инфраструктура Великобритании: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Великобритании. Национальная стратегия кибербезопасности Канады. Критическая информационная инфраструктура Канады: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Канады. Национальная стратегия кибербезопасности Австралии. Критическая информационная инфраструктура Австралии: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Австралии. Национальная стратегия кибербезопасности Новой Зеландии. Критическая информационная инфраструктура Новой Зеландии: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Новой Зеландии. Национальная стратегия кибербезопасности Индии. Критическая информационная инфраструктура Индии: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Индии. Законодательство Индии в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия

кибербезопасности КНР. Критическая информационная инфраструктура КНР: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности КНР. Законодательство КНР в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности Южной Кореи. Критическая информационная инфраструктура Южной Кореи: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Южной Кореи. Законодательство Южной Кореи в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности Японии. Критическая информационная инфраструктура Японии: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности Японии. Законодательство Японии в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности государств Юго-Восточной Азии. Критическая информационная инфраструктура государств Юго-Восточной Азии: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности государств Юго-Восточной Азии. Законодательство государств Юго-Восточной Азии в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности государств Ближнего Востока. Критическая информационная инфраструктура государств Ближнего Востока: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности государств Ближнего Востока. Законодательство государств Ближнего Востока в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных. Национальная стратегия кибербезопасности государств Магриба. Критическая информационная инфраструктура государств Магриба: понятие, объекты, субъекты. Институциональный механизм обеспечения безопасности государств Магриба. Законодательство государств Магриба в области персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Государственный контроль и надзор за обработкой персональных данных. Ответственность за нарушение законодательства в области персональных данных.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция-дискуссия (проблемная лекция), практической занятие, перевернутый класс, собеседование, доклад, творческое задание.

Виды самостоятельной подготовки студентов по теме: подготовка к лекции-дискуссии (проблемной лекции), перевернутому классу, собеседованию, подготовка доклада и творческого задания путем изучения основной и дополнительной литературы.

*Тема 4 Региональные механизмы обеспечения кибербезопасности.*

Содержание темы: Шанхайская организация сотрудничества (ШОС). Ассоциация государств Юго-Восточной Азии (АСЕАН). Европейский Союз (ЕС). Организация Североатлантического договора (НАТО).

Формы и методы проведения занятий по теме, применяемые образовательные

технологии: лекция-дискуссия (проблемная лекция), заключительная лекция, перевернутый класс (на лекциях о других странах), практическое занятие, собеседование, доклад, творческое задание.

Виды самостоятельной подготовки студентов по теме: подготовка к лекции-дискуссии (проблемной лекции), перевернутому классу, собеседованию, подгтовка доклада и выполнение творческого задания путем изучения основной и дополнительной литературы.

## 5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

### 5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Подготовка к лекционным темам, определенным в рабочей программе учебной дисциплины, осуществляется студентами перед запланированной лекцией, определенной учебным расписанием. Подготовка к лекции должна носить общий ознакомительный характер, для выявления проблемного поля темы лекции и обеспечения обратной связи студент – преподаватель. Темы для подготовки к практическим (семинарским) занятиям установлены программой. Подготовка к практическим (семинарским) занятиям предполагает самостоятельный анализ лекционного материала, основной и дополнительной литературы, дополнительных теоретических и практических источников. Конкретная тематика творческих заданий, примерные образцы кейс-задач, вопросы для собеседования по темам содержатся в фонде оценочных средств, входящем в структуру УМК дисциплины и расположенных в электронном виде в разделе «Электронное хранилище материалов». Самостоятельная работа студента состоит из комплекса общих и индивидуальных заданий. В этот комплекс входит самостоятельная подготовка студента к лекциям, семинарским занятиям, а также выполнение творческих заданий.

В процессе изучения учебной дисциплины предполагается изучение и конспектирование первоисточников: материалов периодической печати, научной и учебной литературы, письменный анализ нормативных актов и комментариев к ним.

Для подготовки к лекционному и семинарскому занятию студентом используются такие формы внеаудиторной работы, как реферирование.

Подготовка к лекции позволяет студентам активно и углубленно усваивать получаемы материал, участвовать в интерактивных формах лекции – «лекция-дискуссия», «перевернутый класс» и т.п. Формирование во время лекционных занятий режима «обратной связи» студенческой аудитории и лектора активизирует внимание обучающихся, создает их заинтересованность в изучении предмета. Проведение лекции также предполагает не только объяснение студентам лекционного материала, но и фиксирование ключевой информации в конспектах лекций. С этой целью преподавателем заранее определяется ключевая информация по предмету, которая подается в виде разъясняющего текста, определений, схем. Лекционный материал сопровождается мультимедийными технологиями - наглядным видео, аудио и презентационным материалом, содержащемся в УМК дисциплины.

Использование данного метода предполагает построение лекции как диалогического общения преподавателя со студентами. Во внутреннем диалоге студенты вместе с преподавателем ставят вопросы и отвечают на них или фиксируют вопросы в конспекте для последующего выяснения в ходе самостоятельных заданий, индивидуальной консультации с преподавателем или же обсуждения с другими студентами, а также на семинаре.

Для диалогического включения преподавателя со студентами необходимы следующие условия:

- преподаватель входит в контакт со студентами не как «законодатель», а как собеседник, пришедший на лекцию «поделиться» с ними своим личностным

содержанием;

- преподаватель не только признает право студента на собственное суждение, но и заинтересован в нем;
- новое знание выглядит истинным не только в силу авторитета преподавателя, ученого или автора учебника, но и в силу доказательства его истинности системой рассуждений;
- материал лекции включает обсуждение различных точек зрения на решение учебных проблем, воспроизводит логику развития науки, ее содержания, показывает способы разрешения объективных противоречий в истории науки;
- общение со студентами строится таким образом, чтобы подвести их к самостоятельным выводам, сделать соучастниками процесса подготовки, поиска и нахождения путей разрешения противоречий, созданных самим же преподавателем;
- преподаватель строит вопросы к вводимому материалу и отвечает на них, вызывает вопросы у студентов и стимулирует самостоятельный поиск ответов на них по ходу лекции. Добивается того, что студент думает совместно с ним.

Проблемные вопросы — это вопросы, ответ на которые не содержится ни в прежних знаниях студентов, ни в наличной предъявляемой информации (запись на доске, таблицы на стене и т.п.) и которые вызывают интеллектуальные затруднения у студентов. Проблемные вопросы содержат в себе еще не раскрытую проблему, область неизвестного, новые знания, для добывания которых необходимо какое-то интеллектуальное действие, определенный целенаправленный мыслительный процесс.

Доклад представляет собой продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-исследовательской темы. Доклады готовятся на лекционные занятия по соответствующей теме учебной дисциплины в рамках использования образовательной технологии «перевернутый класс». За две недели до лекции преподаватель определяет группы студентов (как правило, в составе 3-4 человек), которые будут представлять подготовленные доклады по теме дисциплины на лекционном занятии. При подготовке к занятию группы студентов получают у преподавателя списки обязательной и рекомендованной литературы с детальным планом предстоящего доклада.

Доклад готовится в письменной форме и оформляется в соответствии с требованиями, установленными Стандартом СК-СТО-ТР-04-1.005-2015 «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам. Структура и правила оформления», утвержденным приказом ректора ВГУЭС от 29.01.2015 №55.

Для выступления на лекционном занятии группа докладчиков готовит мультимедийную презентацию доклада, оформленную в соответствии со Стандартом СТО 1.219-2008 «Система вузовской учебной документации. Электронные дополнительные учебные материалы. Мультимедийные презентации учебного курса. Структура и форма представления», введенным в действие 20.04.2008.

Продолжительность выступления с докладом и ответов на вопросы аудитории зависит от общего количества докладов, представленных для обсуждения на лекционном занятии. Группа студентов-докладчиков обязана продемонстрировать умения и навыки, на формирование которых было нацелено выполнение данного задания, а также показать отличное владение материалом.

При подготовке группового и/или индивидуального творческого задания 1 студент должен проработать материалы лекционных занятий и провести поиск в средствах массовой информации с целью сбора и обобщения представленного фактического материала с последующим обзором. Творческое задание выполняется в форме аналитической записки и оформляется в соответствии с требованиями, установленными Стандартом СК-СТО-ТР-04-1.005-2015 «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам. Структура и правила оформления», утвержденным приказом ректора

ВГУЭС от 29.01.2015 №55. На практическом занятии студенты защищают результаты аналитической работы и обсуждают проблемные вопросы.

Выполнение творческого задания 2 осуществляется студентом индивидуально по согласованной с преподавателем теме. Студент должен проработать материалы лекционных занятий и провести поиск в средствах массовой информации с целью сбора и обобщения представленного фактического материала с последующим обзором. Творческое задание выполняется в форме аналитической записки и оформляется в соответствии с требованиями, установленными Стандартом СК-СТО-ТР-04-1.005-2015 «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам. Структура и правила оформления», утвержденным приказом ректора ВГУЭС от 29.01.2015 №55. Во время промежуточной аттестации студент должен защитить результаты аналитической работы.

Практическое (семинарское) занятие проводится с целью закрепления знаний, полученных в ходе освоения лекционного материала, выработки первичных профессиональных навыков по изучаемому курсу, решения кейс-задач, а также с целью контроля по освоению пройденного студентами материала.

Перечень вопросов для подготовки к собеседованию и решению кейс-задач определен рабочей программой.

При подготовке к практическим занятиям студентам необходимо придерживаться следующих рекомендаций:

- ознакомиться с тематическим планом дисциплины;

- изучить содержание темы предстоящего практического занятия по предложенным источникам;

- составить конспект предстоящего занятия, используя предлагаемый план и рекомендованные источники;

- зафиксировать вопросы, возникшие в процессе подготовки к занятию.

Подготовка к практическим занятиям предполагает работу с учебной и научной литературой.

При подготовке к лекциям и практическим занятиям использование источников литературы, рекомендованных для соответствующих дидактических единиц, является обязательным условием успешного освоения профессиональных компетенций. В разделе «основная литература» студентам предлагается ознакомиться с базовыми учебными источниками, обеспечивающими необходимый уровень освоения теоретического материала. При этом студентом могут быть использованы и иные альтернативные источники, рекомендуется также проведение сравнительного анализа позиций и взглядов авторов источников, указанных в рабочей программе и найденных самостоятельно. В случае возникающих логических противоречий, выявления неточностей, связанных с разными учебными источниками, необходимо обратится к преподавателю за консультацией. Раздел «дополнительная литература» также содержит источники, обязательные для аудиторной и внеаудиторной работы как теоретического плана, так и конкретных нормативно-правовых актов, судебной практики и т.п. Ознакомление с ними формирует углубленные знания студентов о дисциплине, позволяет сформировать аналитические навыки и практические знания нормативно-правового регулирования.

### 5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме

электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

## 6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

## 7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

### *7.1 Основная литература*

1. Бартош А. А. ОСНОВЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ. ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ. Учебное пособие для бакалавриата и специалитета [Электронный ресурс] , 2019 - 247 - Режим доступа: https://urait.ru/book/osnovy-mezhdunarodnoy-bezopasnosti-organizacii-obespecheniya-mezhdunarodnoy-bezopasnosti-441405

2. Демидов В.В. Информационно-аналитическая работа в международных отношениях : Учебное пособие [Электронный ресурс] : Инфра-М , 2020 - 369 - Режим доступа: https://znanium.com/catalog/document?id=347712

3. Отв. ред. Каламкарян Р. А. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С ПРЕСТУПНОСТЬЮ. Учебник для академического бакалавриата [Электронный ресурс] , 2019 - 349 - Режим доступа: https://urait.ru/book/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-prestupnostyu-432984

### *7.2 Дополнительная литература*

1. Аверьянов Г. С., Яковлев А. Б. Основы теории автоматического управления : Научные монографии [Электронный ресурс] - Москва : Юнити , 2016 - 235 - Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=446953

2. АСЕАН – движущая сила региональной интеграции в Азии : Монография [Электронный ресурс] : НИЦ ИНФРА-М , 2018 - 256 - Режим доступа: https://znanium.com/catalog/document?id=303282

### *7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):*

1. Association of Southeast Asian Nations (ASEAN). - Режим доступа: https://asean.org/
2. European Union Agency for Cybersecurity (ENISA). - Режим доступа: https://www.enisa.europa.eu/
3. North Atlantic Treaty Organization (NATO). - Режим доступа: https://www.nato.int/

4. Справочная правовая система «КонсультантПлюс» - Режим доступа: http://www.consultant.ru/

5. Шанхайская организация сотрудничества (ШОС). - Режим доступа: http://rus.sectsco.org/

6. Электронная библиотечная система «Университетская библиотека онлайн» - Режим доступа: http://biblioclub.ru/

7. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/

8. Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/

9. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/

10. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

## 8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Ноутбук Honor MagicBook 14"

Программное обеспечение:

· VMware Horizon ViewStandard
· Adobe Reader 10 Russian
· Microsoft Office Professional Plus 2013 Russian
· Microsoft Windows 7 Ultimate Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ПРАВА

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

# МЕЖДУНАРОДНЫЙ И НАЦИОНАЛЬНЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Направление и направленность (профиль)

41.03.05 Международные отношения. Международные отношения

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2023

## 1 Перечень формируемых компетенций

| Название ОПОП ВО, сокращенное | Код и формулировка компетенции | Код и формулировка индикатора достижения компетенции |
|---|---|---|
| 41.03.05 «Международные отношения» (Б-МО) | ПКВ-1 : Способен использовать нормы и принципы международного права в качестве регуляторов международных отношений | ПКВ-1.3к : Дает оценку деятельности участников международных отношений в сфере международной безопасности и квалифицированные заключения и консультации в сфере информационной безопасности |

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

## 2 Показатели оценивания планируемых результатов обучения

**Компетенция ПКВ-1** «Способен использовать нормы и принципы международного права в качестве регуляторов международных отношений»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

| Код и формулировка индикатора достижения компетенции | Результаты обучения по дисциплине | | | Критерии оценивания результатов обучения |
|---|---|---|---|---|
| | Код рез-та | Тип рез-та | Результат | |
| ПКВ-1.3к : Дает оценку деятельности участников международных отношений в сфере международной безопасности и квалифицированные заключения и консультации в сфере информационной безопасности | РД1 | Знание | структуры международных и национальных механизмов обеспечения кибербезопасности | полностью характеризует структуру механизмов |
| | РД1 | Умение | анализировать содержание национальных и международных стандартов обеспечения кибербезопасности | использование системно-структурного подхода к анализу |
| | РД1 | Навык | определения преимуществ и недостатков международного и национальных механизмов обеспечения кибербезопасности | аргументированный ответ |

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

## 3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

| Контролируемые планируемые резу | Контролируемые темы | Наименование оценочного средства и представление его в ФОС |
|---|---|---|

| льтаты обучения | | дисциплины | Текущий контроль | Промежуточная ат тестация |
|---|---|---|---|---|
| Очная форма обучения | | | | |
| РД1 | Знание : структуры меж дународных и национал ьных механизмов обеспе чения кибербезопасност и | 1.1. Информационная бе зопасность и кибербезоп асность | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| | | 1.2. Международный ме ханизм обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| | | 1.3. Национальные меха низмы обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| | | 1.4. Региональные меха низмы обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| РД1 | Умение : анализировать содержание национальн ых и международных ст андартов обеспечения к ибербезопасности | 1.2. Международный ме ханизм обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| | | 1.3. Национальные меха низмы обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| | | 1.4. Региональные меха низмы обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |
| | | | Собеседование | Зачет в письменно й форме |
| РД1 | Навык : определения пре имуществ и недостатков международного и наци ональных механизмов о беспечения кибербезопа сности | 1.2. Международный ме ханизм обеспечения киб ербезопасности | Доклад, сообщени е | Зачет в письменно й форме |
| | | | Разноуровневые за дачи и задания | Зачет в письменно й форме |

| | | | | |
|---|---|---|---|---|
| | | | Собеседование | Зачет в письменной форме |
| | | 1.3. Национальные механизмы обеспечения кибербезопасности | Доклад, сообщение | Зачет в письменной форме |
| | | | Разноуровневые задачи и задания | Зачет в письменной форме |
| | | | Собеседование | Зачет в письменной форме |
| | | 1.4. Региональные механизмы обеспечения кибербезопасности | Доклад, сообщение | Зачет в письменной форме |
| | | | Разноуровневые задачи и задания | Зачет в письменной форме |
| | | | Собеседование | Зачет в письменной форме |

## 4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

| Вид учебной деятельности | Оценочное средство | | | | |
|---|---|---|---|---|---|
| | Собеседование | Доклад | Творческое задание | Зачет в письменной форме | Итого |
| Лекции | 3 | 3 | | | 6 |
| Практические занятия | | | 3 | | 3 |
| Самостоятельная работа | 2 | 2 | 2 | | 6 |
| Промежуточная аттестация | | | | 100 | 100 |
| Итого | 10 | 45 | 45 | 100 | 100 |

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

| Сумма баллов по дисциплине | Оценка по промежуточной аттестации | Характеристика качества сформированности компетенции |
|---|---|---|
| от 91 до 100 | «зачтено» / «отлично» | Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности. |
| от 76 до 90 | «зачтено» / «хорошо» | Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| от 61 до 75 | «зачтено» / «удовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |
| от 41 до 60 | «не зачтено» / «неудовлетворительно» | У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков. |

| | | |
|---|---|---|
| от 0 до 40 | «не зачтено» / «неудовлетворительно» | Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков. |

## 5 Примерные оценочные средства

### 5.1 Перечень тем докладов, сообщений

1. Национальная стратегия кибербезопасности Российской Федерации.
2. Критическая информационная инфраструктура Российской Федерации: понятие, объекты, субъекты.
3. Институциональный механизм обеспечения безопасности Российской Федерации.
4. Государственная тайна в Российской Федерации: понятие, режим, объекты и субъекты.
5. Общие положения о государственной тайне в Российской Федерации
6. Перечень сведений, составляющих государственную тайну Российской Федерации
7. Отнесение сведений к государственной тайне и их засекречивание в Российской Федерации
8. Рассекречивание сведений и их носителей в Российской Федерации
9. Распоряжение сведениями, составляющими государственную тайну, в Российской Федерации
10. Защита государственной тайны в Российской Федерации
11. Финансирование мероприятий по защите государственной тайны в Российской Федерации
12. Контроль и надзор за обеспечением защиты государственной тайны в Российской Федерации
13. Законодательство России в области персональных данных.
14. Принципы и условия обработки персональных данных в Российской Федерации.
15. Права субъекта персональных данных в Российской Федерации.
16. Обязанности оператора в Российской Федерации.
17. Государственный контроль и надзор за обработкой персональных данных в Российской Федерации.
18. Ответственность за нарушение законодательства в Российской Федерации в области персональных данных.
19. Национальная стратегия кибербезопасности Сингапура.
20. Критическая информационная инфраструктура Сингапура: понятие, объекты, субъекты.
21. Институциональный механизм обеспечения безопасности Сингапура.
22. Законодательство Сингапура в области персональных данных.
23. Принципы и условия обработки персональных данных в Сингапуре.
24. Права субъекта персональных данных в Сингапуре.
25. Обязанности оператора в Сингапуре.
26. Государственный контроль и надзор за обработкой персональных данных в Сингапуре.
27. Ответственность за нарушение законодательства в Сингапуре в области персональных данных.
28. Национальная стратегия кибербезопасности США.
29. Критическая информационная инфраструктура США: понятие, объекты, субъекты.
30. Институциональный механизм обеспечения безопасности США.
31. Законодательство США в области персональных данных.

32. Принципы и условия обработки персональных данных в США.
33. Права субъекта персональных данных в США.
34. Обязанности оператора в США.
35. Государственный контроль и надзор за обработкой персональных данных в США.
36. Ответственность за нарушение законодательства в США в области персональных данных.
37. Национальная стратегия кибербезопасности Великобритании.
38. Критическая информационная инфраструктура Великобритании: понятие, объекты, субъекты.
39. Институциональный механизм обеспечения безопасности Великобритании.
40. Национальная стратегия кибербезопасности Канады.
41. Критическая информационная инфраструктура Канады: понятие, объекты, субъекты.
42. Институциональный механизм обеспечения безопасности Канады.
43. Национальная стратегия кибербезопасности Австралии.
44. Критическая информационная инфраструктура Австралии: понятие, объекты, субъекты.
45. Институциональный механизм обеспечения безопасности Австралии.
46. Национальная стратегия кибербезопасности Новой Зеландии.
47. Критическая информационная инфраструктура Новой Зеландии: понятие, объекты, субъекты.
48. Институциональный механизм обеспечения безопасности Новой Зеландии.
49. Национальная стратегия кибербезопасности государств Европы.
50. Критическая информационная инфраструктура государств Европы: понятие, объекты, субъекты.
51. Институциональный механизм обеспечения безопасности государств Европы.
52. Национальная стратегия кибербезопасности Индии.
53. Критическая информационная инфраструктура Индии: понятие, объекты, субъекты.
54. Институциональный механизм обеспечения безопасности Индии.
55. Законодательство Индии в области персональных данных.
56. Принципы и условия обработки персональных данных в Индии.
57. Права субъекта персональных данных в Индии.
58. Обязанности оператора в Индии.
59. Государственный контроль и надзор за обработкой персональных данных в Индии.
60. Ответственность за нарушение законодательства в Индии в области персональных данных.
61. Национальная стратегия кибербезопасности КНР.
62. Критическая информационная инфраструктура КНР: понятие, объекты, субъекты.
63. Институциональный механизм обеспечения безопасности КНР.
64. Национальная стратегия кибербезопасности Южной Кореи.
65. Критическая информационная инфраструктура Южной Кореи: понятие, объекты, субъекты.
66. Институциональный механизм обеспечения безопасности Южной Кореи.
67. Национальная стратегия кибербезопасности Японии.
68. Критическая информационная инфраструктура Японии: понятие, объекты, субъекты.
69. Институциональный механизм обеспечения безопасности Японии.
70. Законодательство государств Северо-восточной Азии в области персональных данных.
71. Принципы и условия обработки персональных данных в государствах Северо-восточной Азии.

72. Права субъекта персональных данных в государствах Северо-восточной Азии.

73. Обязанности оператора в государствах Северо-восточной Азии

74. Государственный контроль и надзор за обработкой персональных данных в государствах Северо-восточной Азии.

75. Ответственность за нарушение законодательства в области персональных данных в государствах Северо-восточной Азии

76. Национальная стратегия кибербезопасности государств Юго-Восточной Азии.

77. Критическая информационная инфраструктура государств Юго-Восточной Азии: понятие, объекты, субъекты.

78. Институциональный механизм обеспечения безопасности государств Юго-Восточной Азии.

79. Законодательство государств Юго-Восточной Азии в области персональных данных.

80. Принципы и условия обработки персональных данных в государствах Юго-Восточной Азии.

81. Права субъекта персональных данных в государствах Юго-Восточной Азии.

82. Обязанности оператора в государствах Юго-Восточной Азии

83. Государственный контроль и надзор за обработкой персональных данных в государствах Юго-Восточной Азии.

84. Ответственность за нарушение законодательства в области персональных данных в государствах Юго-Восточной Азии

85. Национальная стратегия кибербезопасности государств Ближнего Востока.

86. Критическая информационная инфраструктура государств Ближнего Востока: понятие, объекты, субъекты.

87. Институциональный механизм обеспечения безопасности государств Ближнего Востока.

88. Национальная стратегия кибербезопасности государств Магриба.

89. Критическая информационная инфраструктура государств Магриба: понятие, объекты, субъекты.

90. Институциональный механизм обеспечения безопасности государств Магриба.

91. Законодательство государств Ближнего Востока и Магриба в области персональных данных.

92. Принципы и условия обработки персональных данных в государствах Ближнего Востока и Магриба.

93. Права субъекта персональных данных в государствах Ближнего Востока и Магриба.

94. Обязанности оператора в государствах Ближнего Востока и Магриба

95. Государственный контроль и надзор за обработкой персональных данных в государствах Ближнего Востока и Магриба.

96. Ответственность за нарушение законодательства в области персональных данных в государствах Ближнего Востока и Магриба.

*Краткие методические указания*

Доклад представляет собой продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-исследовательской темы. Доклады готовятся на лекционные занятия по соответствующей теме учебной дисциплины в рамках использования образовательной технологии «перевернутый класс». За две недели до лекции преподаватель определяет группы студентов (как правило, в составе 3-4 человек), которые будут представлять подготовленные доклады по теме дисциплины на лекционном занятии. При подготовке к занятию группы студентов получают у преподавателя списки обязательной и рекомендованной литературы с детальным планом предстоящего доклада.

Доклад готовится в письменной форме и оформляется в соответствии с требованиями, установленными Стандартом СК-СТО-ТР-04-1.005-2015 «Требования к оформлению

текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам. Структура и правила оформления», утвержденным приказом ректора ВГУЭС от 29.01.2015 №55.

Для выступления на лекционном занятии группа докладчиков готовит мультимедийную презентацию доклада, оформленную в соответствии со Стандартом СТО 1.219-2008 «Система вузовской учебной документации. Электронные дополнительные учебные материалы. Мультимедийные презентации учебного курса. Структура и форма представления», введенным в действие 20.04.2008.

Продолжительность выступления с докладом и ответов на вопросы аудитории зависит от общего количества докладов, представленных для обсуждения на лекционном занятии. Группа студентов-докладчиков обязана продемонстрировать умения и навыки, на формирование которых было нацелено выполнение данного задания, а также показать отличное владение материалом.

*Шкала оценки*

| Оценка | Баллы | Описание |
|---|---|---|
| 5 | 5 | студент представил отличное исполнение с незначительным числом ошибок |
| 4 | 4 | студент показал уровень владения материалом выше среднего с несколькими ошибками |
| 3 | 3 | в целом правильно, но со значительным количеством недостатков |
| 2 | 0 | в целом правильное исполнение с критическим количеством существенных ошибок |

**5.2 Вопросы к зачету (письменная форма)**

Тема 1. Информационная безопасность и кибербезопасность

1. Понятие информации
2. Идея информационного общества
3. Теоретические концепции информационного общества
4. Информатизация и глобализация
5. Основные направления информационного противоборства
6. Новые объекты информационной безопасности
7. Соотношение понятий «информационная безопасность» и «кибербезопасность»

Тема 2. Международный механизм обеспечения кибербезопасности

1. Основные аспекты информационной безопасности
2. Информация и безопасность, информационная безопасность: определение понятий
3. Эволюция международно-правового регулирования информационных отношений с точки зрения обеспечения информационной безопасности
4. Стратегия в области информационно-коммуникационных технологий (резолюции ГА ООН)
5. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур (резолюции ГА ООН)
6. Использование информационно-коммуникационных технологий в целях развития (резолюции ГА ООН)
7. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности (резолюции ГА ООН)
8. Борьба с преступным использованием информационных технологий (резолюции ГА ООН)

Тема 3. Национальные механизмы обеспечения кибербезопасности

1. Национальная стратегия кибербезопасности Российской Федерации.
2. Критическая информационная инфраструктура Российской Федерации: понятие, объекты, субъекты.
3. Институциональный механизм обеспечения безопасности Российской Федерации.
4. Государственная тайна в Российской Федерации: понятие, режим, объекты и субъекты.
5. Общие положения о государственной тайне в Российской Федерации
6. Перечень сведений, составляющих государственную тайну Российской Федерации

7. Отнесение сведений к государственной тайне и их засекречивание в Российской Федерации
8. Рассекречивание сведений и их носителей в Российской Федерации
9. Распоряжение сведениями, составляющими государственную тайну, в Российской Федерации
10. Защита государственной тайны в Российской Федерации
11. Финансирование мероприятий по защите государственной тайны в Российской Федерации
12. Контроль и надзор за обеспечением защиты государственной тайны в Российской Федерации
13. Законодательство России в области персональных данных.
14. Принципы и условия обработки персональных данных в Российской Федерации.
15. Права субъекта персональных данных в Российской Федерации.
16. Обязанности оператора в Российской Федерации.
17. Государственный контроль и надзор за обработкой персональных данных в Российской Федерации.
18. Ответственность за нарушение законодательства в Российской Федерации в области персональных данных.
19. Национальная стратегия кибербезопасности Сингапура.
20. Критическая информационная инфраструктура Сингапура: понятие, объекты, субъекты.
21. Институциональный механизм обеспечения безопасности Сингапура.
22. Законодательство Сингапура в области персональных данных.
23. Принципы и условия обработки персональных данных в Сингапуре.
24. Права субъекта персональных данных в Сингапуре.
25. Обязанности оператора в Сингапуре.
26. Государственный контроль и надзор за обработкой персональных данных в Сингапуре.
27. Ответственность за нарушение законодательства в Сингапуре в области персональных данных.
28. Национальная стратегия кибербезопасности США.
29. Критическая информационная инфраструктура США: понятие, объекты, субъекты.
30. Институциональный механизм обеспечения безопасности США.
31. Законодательство США в области персональных данных.
32. Принципы и условия обработки персональных данных в США.
33. Права субъекта персональных данных в США.
34. Обязанности оператора в США.
35. Государственный контроль и надзор за обработкой персональных данных в США.
36. Ответственность за нарушение законодательства в США в области персональных данных.
37. Национальная стратегия кибербезопасности Великобритании.
38. Критическая информационная инфраструктура Великобритании: понятие, объекты, субъекты.
39. Институциональный механизм обеспечения безопасности Великобритании.
40. Национальная стратегия кибербезопасности Канады.
41. Критическая информационная инфраструктура Канады: понятие, объекты, субъекты.
42. Институциональный механизм обеспечения безопасности Канады.
43. Национальная стратегия кибербезопасности Австралии.
44. Критическая информационная инфраструктура Австралии: понятие, объекты, субъекты.
45. Институциональный механизм обеспечения безопасности Австралии.

46. Национальная стратегия кибербезопасности Новой Зеландии.

47. Критическая информационная инфраструктура Новой Зеландии: понятие, объекты, субъекты.

48. Институциональный механизм обеспечения безопасности Новой Зеландии.

49. Национальная стратегия кибербезопасности государств Европы.

50. Критическая информационная инфраструктура государств Европы: понятие, объекты, субъекты.

51. Институциональный механизм обеспечения безопасности государств Европы.

52. Национальная стратегия кибербезопасности Индии.

53. Критическая информационная инфраструктура Индии: понятие, объекты, субъекты.

54. Институциональный механизм обеспечения безопасности Индии.

55. Законодательство Индии в области персональных данных.

56. Принципы и условия обработки персональных данных в Индии.

57. Права субъекта персональных данных в Индии.

58. Обязанности оператора в Индии.

59. Государственный контроль и надзор за обработкой персональных данных в Индии.

60. Ответственность за нарушение законодательства в Индии в области персональных данных.

61. Национальная стратегия кибербезопасности КНР.

62. Критическая информационная инфраструктура КНР: понятие, объекты, субъекты.

63. Институциональный механизм обеспечения безопасности КНР.

64. Национальная стратегия кибербезопасности Южной Кореи.

65. Критическая информационная инфраструктура Южной Кореи: понятие, объекты, субъекты.

66. Институциональный механизм обеспечения безопасности Южной Кореи.

67. Национальная стратегия кибербезопасности Японии.

68. Критическая информационная инфраструктура Японии: понятие, объекты, субъекты.

69. Институциональный механизм обеспечения безопасности Японии.

70. Законодательство государств Северо-восточной Азии в области персональных данных.

71. Принципы и условия обработки персональных данных в государствах Северо-восточной Азии.

72. Права субъекта персональных данных в государствах Северо-восточной Азии.

73. Обязанности оператора в государствах Северо-восточной Азии

74. Государственный контроль и надзор за обработкой персональных данных в государствах Северо-восточной Азии.

75. Ответственность за нарушение законодательства в области персональных данных в государствах Северо-восточной Азии

76. Национальная стратегия кибербезопасности государств Юго-Восточной Азии.

77. Критическая информационная инфраструктура государств Юго-Восточной Азии: понятие, объекты, субъекты.

78. Институциональный механизм обеспечения безопасности государств Юго-Восточной Азии.

79. Законодательство государств Юго-Восточной Азии в области персональных данных.

80. Принципы и условия обработки персональных данных в государствах Юго-Восточной Азии.

81. Права субъекта персональных данных в государствах Юго-Восточной Азии.

82. Обязанности оператора в государствах Юго-Восточной Азии

83. Государственный контроль и надзор за обработкой персональных данных в

государствах Юго-Восточной Азии.

84. Ответственность за нарушение законодательства в области персональных данных в государствах Юго-Восточной Азии

85. Национальная стратегия кибербезопасности государств Ближнего Востока.

86. Критическая информационная инфраструктура государств Ближнего Востока: понятие, объекты, субъекты.

87. Институциональный механизм обеспечения безопасности государств Ближнего Востока.

88. Национальная стратегия кибербезопасности государств Магриба.

89. Критическая информационная инфраструктура государств Магриба: понятие, объекты, субъекты.

90. Институциональный механизм обеспечения безопасности государств Магриба.

91. Законодательство государств Ближнего Востока и Магриба в области персональных данных.

92. Принципы и условия обработки персональных данных в государствах Ближнего Востока и Магриба.

93. Права субъекта персональных данных в государствах Ближнего Востока и Магриба.

94. Обязанности оператора в государствах Ближнего Востока и Магриба

95. Государственный контроль и надзор за обработкой персональных данных в государствах Ближнего Востока и Магриба.

96. Ответственность за нарушение законодательства в области персональных данных в государствах Ближнего Востока и Магриба.

Тема 4. Региональные механизмы обеспечения кибербезопасности

1. Шанхайская организация сотрудничества (ШОС).
2. Организация Североатлантического договора (НАТО).
3. Европейский Союз (ЕС).
4. Ассоциация государств Юго-Восточной Азии (АСЕАН).

*Краткие методические указания*

При подготовке к зачету студент обязан проработать нормативно-правовые источники по темам дисциплины, основную и дополнительную литературу (с обязательным конспектированием изучаемого материала).

*Шкала оценки*

| Оценка | Баллы | Описание |
|---|---|---|
| 5 | 91-100 | студент представил отличное исполнение с незначительным числом ошибок |
| 4 | 76-90 | студент показал уровень владения материалом выше среднего с несколькими ошибками |
| 3 | 61-75 | в целом правильно, но со значительным количеством недостатков |
| 2 | 0 | в целом правильное исполнение с критическим количеством существенных ошибок |

**5.3 Примерный перечень вопросов по темам**

Тема 1. Информационная безопасность и кибербезопасность

1. Понятие информации
2. Идея информационного общества
3. Теоретические концепции информационного общества
4. Информатизация и глобализация
5. Основные направления информационного противоборства
6. Новые объекты информационной безопасности
7. Соотношение понятий «информационная безопасность» и «кибербезопасность»

Тема 2. Международный механизм обеспечения кибербезопасности

1. Основные аспекты информационной безопасности
2. Информация и безопасность, информационная безопасность: определение понятий
3. Эволюция международно-правового регулирования информационных отношений с

точки зрения обеспечения информационной безопасности

4. Стратегия в области информационно-коммуникационных технологий (резолюции ГА ООН)

5. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур (резолюции ГА ООН)

6. Использование информационно-коммуникационных технологий в целях развития (резолюции ГА ООН)

7. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности (резолюции ГА ООН)

8. Борьба с преступным использованием информационных технологий (резолюции ГА ООН)

Тема 3. Национальные механизмы обеспечения кибербезопасности

1. Национальная стратегия кибербезопасности Российской Федерации.
2. Критическая информационная инфраструктура Российской Федерации: понятие, объекты, субъекты.
3. Институциональный механизм обеспечения безопасности Российской Федерации.
4. Государственная тайна в Российской Федерации: понятие, режим, объекты и субъекты.
5. Общие положения о государственной тайне в Российской Федерации
6. Перечень сведений, составляющих государственную тайну Российской Федерации
7. Отнесение сведений к государственной тайне и их засекречивание в Российской Федерации
8. Рассекречивание сведений и их носителей в Российской Федерации
9. Распоряжение сведениями, составляющими государственную тайну, в Российской Федерации

10. Защита государственной тайны в Российской Федерации

11. Финансирование мероприятий по защите государственной тайны в Российской Федерации

12. Контроль и надзор за обеспечением защиты государственной тайны в Российской Федерации

13. Законодательство России в области персональных данных.

14. Принципы и условия обработки персональных данных в Российской Федерации.

15. Права субъекта персональных данных в Российской Федерации.

16. Обязанности оператора в Российской Федерации.

17. Государственный контроль и надзор за обработкой персональных данных в Российской Федерации.

18. Ответственность за нарушение законодательства в Российской Федерации в области персональных данных.

19. Национальная стратегия кибербезопасности Сингапура.

20. Критическая информационная инфраструктура Сингапура: понятие, объекты, субъекты.

21. Институциональный механизм обеспечения безопасности Сингапура.

22. Законодательство Сингапура в области персональных данных.

23. Принципы и условия обработки персональных данных в Сингапуре.

24. Права субъекта персональных данных в Сингапуре.

25. Обязанности оператора в Сингапуре.

26. Государственный контроль и надзор за обработкой персональных данных в Сингапуре.

27. Ответственность за нарушение законодательства в Сингапуре в области персональных данных.

28. Национальная стратегия кибербезопасности США.

29. Критическая информационная инфраструктура США: понятие, объекты, субъекты.

30. Институциональный механизм обеспечения безопасности США.
31. Законодательство США в области персональных данных.
32. Принципы и условия обработки персональных данных в США.
33. Права субъекта персональных данных в США.
34. Обязанности оператора в США.
35. Государственный контроль и надзор за обработкой персональных данных в США.
36. Ответственность за нарушение законодательства в США в области персональных данных.
37. Национальная стратегия кибербезопасности Великобритании.
38. Критическая информационная инфраструктура Великобритании: понятие, объекты, субъекты.
39. Институциональный механизм обеспечения безопасности Великобритании.
40. Национальная стратегия кибербезопасности Канады.
41. Критическая информационная инфраструктура Канады: понятие, объекты, субъекты.
42. Институциональный механизм обеспечения безопасности Канады.
43. Национальная стратегия кибербезопасности Австралии.
44. Критическая информационная инфраструктура Австралии: понятие, объекты, субъекты.
45. Институциональный механизм обеспечения безопасности Австралии.
46. Национальная стратегия кибербезопасности Новой Зеландии.
47. Критическая информационная инфраструктура Новой Зеландии: понятие, объекты, субъекты.
48. Институциональный механизм обеспечения безопасности Новой Зеландии.
49. Национальная стратегия кибербезопасности государств Европы.
50. Критическая информационная инфраструктура государств Европы: понятие, объекты, субъекты.
51. Институциональный механизм обеспечения безопасности государств Европы.
52. Национальная стратегия кибербезопасности Индии.
53. Критическая информационная инфраструктура Индии: понятие, объекты, субъекты.
54. Институциональный механизм обеспечения безопасности Индии.
55. Законодательство Индии в области персональных данных.
56. Принципы и условия обработки персональных данных в Индии.
57. Права субъекта персональных данных в Индии.
58. Обязанности оператора в Индии.
59. Государственный контроль и надзор за обработкой персональных данных в Индии.
60. Ответственность за нарушение законодательства в Индии в области персональных данных.
61. Национальная стратегия кибербезопасности КНР.
62. Критическая информационная инфраструктура КНР: понятие, объекты, субъекты.
63. Институциональный механизм обеспечения безопасности КНР.
64. Национальная стратегия кибербезопасности Южной Кореи.
65. Критическая информационная инфраструктура Южной Кореи: понятие, объекты, субъекты.
66. Институциональный механизм обеспечения безопасности Южной Кореи.
67. Национальная стратегия кибербезопасности Японии.
68. Критическая информационная инфраструктура Японии: понятие, объекты, субъекты.
69. Институциональный механизм обеспечения безопасности Японии.
70. Законодательство государств Северо-восточной Азии в области персональных данных.

71. Принципы и условия обработки персональных данных в государствах Северо-восточной Азии.

72. Права субъекта персональных данных в государствах Северо-восточной Азии.

73. Обязанности оператора в государствах Северо-восточной Азии

74. Государственный контроль и надзор за обработкой персональных данных в государствах Северо-восточной Азии.

75. Ответственность за нарушение законодательства в области персональных данных в государствах Северо-восточной Азии

76. Национальная стратегия кибербезопасности государств Юго-Восточной Азии.

77. Критическая информационная инфраструктура государств Юго-Восточной Азии: понятие, объекты, субъекты.

78. Институциональный механизм обеспечения безопасности государств Юго-Восточной Азии.

79. Законодательство государств Юго-Восточной Азии в области персональных данных.

80. Принципы и условия обработки персональных данных в государствах Юго-Восточной Азии.

81. Права субъекта персональных данных в государствах Юго-Восточной Азии.

82. Обязанности оператора в государствах Юго-Восточной Азии

83. Государственный контроль и надзор за обработкой персональных данных в государствах Юго-Восточной Азии.

84. Ответственность за нарушение законодательства в области персональных данных в государствах Юго-Восточной Азии

85. Национальная стратегия кибербезопасности государств Ближнего Востока.

86. Критическая информационная инфраструктура государств Ближнего Востока: понятие, объекты, субъекты.

87. Институциональный механизм обеспечения безопасности государств Ближнего Востока.

88. Национальная стратегия кибербезопасности государств Магриба.

89. Критическая информационная инфраструктура государств Магриба: понятие, объекты, субъекты.

90. Институциональный механизм обеспечения безопасности государств Магриба.

91. Законодательство государств Ближнего Востока и Магриба в области персональных данных.

92. Принципы и условия обработки персональных данных в государствах Ближнего Востока и Магриба.

93. Права субъекта персональных данных в государствах Ближнего Востока и Магриба.

94. Обязанности оператора в государствах Ближнего Востока и Магриба

95. Государственный контроль и надзор за обработкой персональных данных в государствах Ближнего Востока и Магриба.

96. Ответственность за нарушение законодательства в области персональных данных в государствах Ближнего Востока и Магриба.

Тема 4. Региональные механизмы обеспечения кибербезопасности

1. Шанхайская организация сотрудничества (ШОС).
2. Организация Североатлантического договора (НАТО).
3. Европейский Союз (ЕС).
4. Ассоциация государств Юго-Восточной Азии (АСЕАН).

*Краткие методические указания*

При подготовке к собеседованию студент обязан проработать нормативно-правовые источники по теме дисциплины, основную и дополнительную литературу (с обязательным конспектированием изучаемого материала – при собеседовании с преподавателем студент

может использовать свои записи).

*Шкала оценки*

| Оценка | Баллы | Описание |
|---|---|---|
| 5 | 5 | студент представил отличное исполнение с незначительным числом ошибок |
| 4 | 4 | студент показал уровень владения материалом выше среднего с несколькими ошибками |
| 3 | 3 | в целом правильно, но со значительным количеством недостатков |
| 2 | 0 | в целом правильное исполнение с критическим количеством существенных ошибок |

**5.4 Темы групповых и/или индивидуальных творческих заданий**

Подбор фактологического новостного материала по темам учебной дисциплины

*Краткие методические указания*

При подготовке группового и/или индивидуального творческого задания студент должен проработать материалы лекционных занятий и провести поиск в средствах массовой информации с целью сбора и обобщения представленного фактического материала с последующим обзором. Творческое задание выполняется в форме аналитической записки и оформляется в соответствии с требованиями, установленными Стандартом СК-СТО-ТР-04-1.005-2015 «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам. Структура и правила оформления», утвержденным приказом ректора ВГУЭС от 29.01.2015 №55. На практическом занятии студенты защищают результаты аналитической работы и обсуждают проблемные вопросы.

*Шкала оценки*

| Оценка | Баллы | Описание |
|---|---|---|
| 5 | 5 | студент представил отличное исполнение с незначительным числом ошибок |
| 4 | 4 | студент показал уровень владения материалом выше среднего с несколькими ошибками |
| 3 | 3 | в целом правильно, но со значительным количеством недостатков |
| 2 | 0 | в целом правильное исполнение с критическим количеством существенных ошибок |