МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования
**«Российский государственный
университет социальных технологий»**
**(ФГБОУ ИВО «РГУ СоцТех»)**

УТВЕРЖДАЮ

Проректор по образовательной деятельности

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**
**МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ**
образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
Б1.В.ДВ.01.01 «Дисциплины(модули)», Часть, формируемая участниками образовательных отношений, Дисциплины(модули) по выбору

**Профиль подготовки**
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:
Магистр

Форма обучения очная

Курс 2 семестр 3

Москва 2024

**Содержание**

## 1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

**Цель:**

- изучение студентами стандартов в области международного и национального правового регулирования безопасности в информационной сфере.

**Задачи:**

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

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»

Дисциплина относится к части учебного плана, «Дисциплины по выбору»

1.3. Требования к результатам освоения дисциплины

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций:

Профессиональные (ПК) – в соответствии с ФГОС 3++.

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции |
|---|---|
| ПК-6 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС | ПК-6.1 Знает различные методы решения задач при создании экономических информационных систем; методы проектирования автоматизированных и информационных систем для решения прикладных задач; информационные технологии, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции. |
| | ПК-6.2 Умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации; использовать программные средства, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции. |
| | ПК-6.3 Владеет методами описания информационных систем; навыками сбора, формализации и обработки информации; навыками использования инструментальных средств прикладной информатики создания высоконагруженных информационных систем; классами, |

| | |
|---|---|
| | пакетами и возможностями автоматизированных средств обеспечения; навыками работы с информационными технологиями, применяемыми на этапах разработки, производства, испытаний и эксплуатации продукции. |
| ПК-2.<br><br>Способен формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок. | ПК-2.1 Знает основные принципы и этапы построения математических моделей; границы возможностей существующих методов исследования объектов и процессов; модели бизнес-процессов организации для их оценки и последующей оптимизации на предприятиях прикладной области. |
| | ПК-2.2 Умеет обосновывать выбор математического аппарата, применяемого для формализации задач прикладной области; выдвигать гипотезы относительно элементов структуры или поведения систем, по которым существует недостаток исходной информации; принимать допущения относительно элементов структуры или поведения систем, которые требуют упрощенного представления при формальном описании; проектировать информационные процессы и системы с использованием современных инструментальных средств; проектировать инфраструктуру ИС прикладной области. |
| | ПК-2.3 Владеет приемами, применяемыми при формализации задач прикладной области, выполняемой с использованием различного математического аппарата; навыками формализованного описания этапов работы и оптимизации процесса разработки ИС и технологий предприятий прикладной области в условиях неопределенности и риска. |
| ПК-1<br><br>Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях | ПК-1.1 Знает основные подходы, методы в области проектирования и управления информационными системами в прикладных областях; возможности современных инструментальных средств для проектирования и управления информационными системами в прикладных областях; способы представления научно-технической информации. |
| | ПК-1.2 Умеет использовать и развивать методы научных исследований в области проектирования и управления информационными системами в прикладных областях; анализировать иностранные источники в области проектирования и управления ИС в прикладных областях; использовать и развивать методы инструментарий в области проектирования и управления информационными системами в прикладных областях; правильно подготавливать научно-технические отчеты; оформлять результаты исследований в |

| | |
|---|---|
| | виде статей и докладов на научных конференциях в предметной области. |
| | ПК-1.3 Владеет практическими навыками использования и развития инструментальных средств в области проектирования и управления информационными системами в прикладных областях; навыками работы в системах поиска информации, текстовых процессорах, электронных таблицах, базах данных и системах подготовки презентаций. |
| ПК-3<br><br>Способен разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач проектной деятельности | ПК-3.1. Знает языки программирования, библиотеки и пакеты программ; современные методы цифровой обработки изображений и средства компьютерной обработки информации. |
| | ПК-3.2. Умеет анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи. |
| | ПК-3.3. Владеет методами моделирования информационных процессов; навыками работы над проектом в составе группы научных специалистов. |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Международные организации по кибербезопасности » составляет 6 зачетных единиц/216 часов:

| **Вид учебной работы** | **Всего, часов** | **Очная форма** |
|---|---|---|
| | | **Курс,часов** |
| | **Очная форма** | 2 курс, 3 семестр |
| **Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:** | 48 | 48 |
| Лекции (Л) | 14 | 14 |
| Практические занятия (ПЗ) | 34 | 34 |
| Лабораторные работы (ЛР) | | |
| **Самостоятельная работа обучающихся (СР)** | 132 | 132 |
| **Контроль** | 36 | 36 |
| **Промежуточная аттестация (подготовка и сдача), всего:** | | |
| Контрольная работа | | |

| | | |
|---|---|---|
| Курсовая работа | | |
| Зачет | - | - |
| Экзамен | + | + |
| Итого:<br>Общая трудоемкость учебной дисциплины (в часах, зач. ед.) | 216/6 | 216/6 |

2.2. Содержание дисциплины по темам (разделам)

| № п/п | Наименование раздела (темы) | Содержание раздела (тематика занятий) | Формируемые компетенции (индекс) |
|---|---|---|---|
| 1. | Информационная безопасность и кибербезопасность | 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» | ПК-1, ПК-2, ПК-3, ПК-6 |
| 2. | Международный механизм обеспечения кибербезопасности | Основные аспекты информационной безопасности. Информация и безопасность, информационная безопасность: определение понятий. Эволюция международно-правового регулирования информационных отношений с точки зрения обеспечения информационной безопасности | ПК-1, ПК-2, ПК-3, ПК-6 |
| 3 | Национальные механизмы обеспечения кибербезопасности. | 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 | ПК-1, ПК-2, ПК-3, ПК-6 |
| 4 | Региональные механизмы обеспечения кибербезопасности | Шанхайская организация сотрудничества (ШОС). Ассоциация государств Юго-Восточной Азии (АСЕАН). Европейский Союз (ЕС). Организация Североатлантического договора (НАТО) | ПК-1, ПК-2, ПК-3, ПК-6 |

2.3. Разделы дисциплин и виды занятий

| № п/п | Наименование темы дисциплины | Лекционные занятия | Практические занятия | Самостоятельная работа | Контроль | Всего часов | Формы текущего контроля успеваемости |
|---|---|---|---|---|---|---|---|
| 1. | Информационная безопасность и | 3 | 9 | 33 | 9 | 54 | Устный |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | кибербезопасность | | | | | | опрос |
| 2. | Международный механизм обеспечения кибербезопасности | 4 | 8 | 33 | 9 | 54 | Устный опрос |
| 3 | Национальные механизмы обеспечения кибербезопасности. | 4 | 9 | 33 | 9 | 55 | Устный опрос |
| 4 | Региональные механизмы обеспечения кибербезопасности | 3 | 8 | 33 | 9 | 53 | Устный опрос |
| **Экзамен** | | + | | | | | |
| | Итого: | 14 | 34 | 132 | 36 | 216\6 | |

2.4. План самостоятельной работы обучающегося по дисциплине (модулю)
Очная форма обучения

| № | Название разделов и тем | Виды самостоятельной работы | Трудоемкость | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|---|
| 1. | Информационная безопасность и кибербезопасность | Изучение источников | 33 | ПК-1, ПК-2, ПК-3, ПК-6 | Устный опрос |
| 2. | Международный механизм обеспечения кибербезопасности | Составление отчетов | 33 | ПК-1, ПК-2, ПК-3, ПК-6 | Устный опрос |
| 3. | Национальные механизмы обеспечения кибербезопасности. | Составление отчетов | 33 | ПК-1 ,ПК-2, ПК-3, ПК-6 | Устный опрос |
| 4. | Региональные механизмы обеспечения кибербезопасности | Составление отчетов | 33 | ПК-1, ПК-2, ПК-3, ПК-6 | Устный опрос |

## 3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

## 4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

**Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов** (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1 Перечень основной литературы


1. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. - 140 с. - ISBN 978-5-9275-3546-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1308349
2. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736


### 5.2. Перечень дополнительной литературы


1. Сэрра, Э. Кибербезопасность: правила игры : Как руководители и сотрудники влияют на культуру безопасности в компании : практическое руководство / Э. Сэрра. - Москва : Альпина ПРО, 2022. - 189 с. - ISBN 978-5-907470-58-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1905864
2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734
3. *Козырь, Н. С.* Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/545066
4. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). —

ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247

### 5.3. Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

| № п/п | Наименование оборудованных учебных кабинетов, лабораторий | Перечень оборудования и технических средств обучения |
|---|---|---|
| 1. | Лекционная аудитория | Персональный компьютер, мультимедийный проектор |
| 2. | Компьютерный класс | Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет |

## 7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

| **№** | **Критерии оценки** | | | |
|---|---|---|---|---|
| | **«неудовлетворительно»** | **«удовлетворительно»** | **«хорошо»** | **«отлично»** |
| **ЗНАТЬ** | | | | |
| **1** | Студент не знает основные понятия информационной безопасности и кибербезопасности, не понимает особенности международной, национальной и региональной системы кибербезопасности, не имеет представления об организациях отвечающих за обеспечение кибербезопасности, современных | Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о принципах современных информационно-коммуникационных технологий обеспечения кибербезопасности, о понятиях информационной | Студент способен самостоятельно выделять главные положения в изученном материале.<br>Знает принципы современных информационно-коммуникационных технологий обеспечения кибербезопасности, ориентируется в понятиях информационной | Студент знает понятия информационной безопасности и кибербезопасности, понимает сходства и различия международной, национальной и региональной системы кибербезопасности, ориентируется в организациях отвечающих за обеспечение кибербезопасности, современных |

| | | | | |
|---|---|---|---|---|
| | информационно-коммуникационных технологиях, используемых в этой сфере | безопасности и кибербезопасности | безопасности и кибербезопасности, имеет представление о международных, национальных и региональных механизмах обеспечения кибербезопасности | информационно-коммуникационных технологиях, используемых в этой сфере |
| **УМЕТЬ** | | | | |
| **2** | Студент не умеет применять современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использовать новейшие информационно-коммуникационные технологии в своей профессиональной деятельности | Студент испытывает затруднения при применении современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использует информационно-коммуникационные технологии в своей профессиональной деятельности с большими ограничениями (умееет пользоваться основными функциями) | Студент умеет применять современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использовать базовые функции новейших информационно-коммуникационные технологии в своей профессиональной деятельности | Студент умеет применять широкий спектр методов и разных ИКТ в сфере кибербезопасности, различать особенности построения международной, национальной и региональной системы кибербезопасности |
| **ВЛАДЕТЬ** | | | | |
| **3** | Студент не владеет современными технологиями в сфере кибербезопасности, не способен различать особенности международной, национальной и региональной системы кибербезопасности, не владеет навыками использования современных | Студент испытывает трудности с владением современными технологиями в сфере кибербезопасности, путается в описании особенности международной, национальной и региональной системы кибербезопасности, плохо владеет навыками | Студент владеет основными технологиями в сфере кибербезопасности, способен различать особенности международной, национальной и региональной системы кибербезопасности, в целом владеет навыками использования | Студент хорошо владеет основными технологиями в сфере кибербезопасности, отлично ориентируется в особенностях международной, национальной и региональной системы кибербезопасности, отлично владеют навыками |

| | | | | |
|---|---|---|---|---|
| | информационно-коммуникационных технологий в этой сфере | использования современных информационно-коммуникационных технологий в этой сфере | современных информационно-коммуникационных технологий в этой сфере | использования современных информационно-коммуникационных технологий в этой сфере |
| | Компетенции или их части не сформированы. | Компетенции или их части сформированы на базовом уровне. | Компетенции или их части сформированы на среднем уровне. | Компетенции или их части сформированы на высоком уровне. |

## 8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

## 9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос.

Промежуточная аттестация – экзамен

### 9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

### 9.3. Курсовая работа

Не предусмотрено.

### 9.4. Вопросы к зачету

Не предусмотрены

### 9.5. Вопросы к экзамену

1. Информационная безопасность и кибербезопасность
2. Понятие информации
3. Идея информационного общества
4. Теоретические концепции информационного общества
5. Информатизация и глобализация
6. Основные направления информационного противоборства
7. Новые объекты информационной безопасности
8. Соотношение понятий «информационная безопасность» и «кибербезопасность» Основные аспекты информационной безопасности
9. Информация и безопасность, информационная безопасность: определение понятия

10. Эволюция международно-правового регулирования информационных отношений с точки зрения обеспечения информационной безопасности
11. Стратегия в области информационно-коммуникационных технологий (резолюции ГА ООН)
12. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур (резолюции ГА ООН)
13. Использование информационно-коммуникационных технологий в целях развития (резолюции ГА ООН)
14. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности (резолюции ГА ООН)
15. Борьба с преступным использованием информационных технологий (резолюции ГА ООН) Национальная стратегия кибербезопасности Российской Федерации.
16. Критическая информационная инфраструктура Российской Федерации: понятие, объекты, субъекты.
17. Институциональный механизм обеспечения безопасности Российской Федерации. Государственная тайна в Российской Федерации: понятие, режим, объекты и субъекты. Общие положения о государственной тайне в Российской Федерации
18. Перечень сведений, составляющих государственную тайну Российской Федерации Отнесение сведений к государственной тайне и их засекречивание в Российской Федерации
19. Рассекречивание сведений и их носителей в Российской Федерации
20. Распоряжение сведениями, составляющими государственную тайну, в Российской Федерации
21. Защита государственной тайны в Российской Федерации
22. Финансирование мероприятий по защите государственной тайны в Российской Федерации
23. Контроль и надзор за обеспечением защиты государственной тайны в Российской Федерации
24. Законодательство России в области персональных данных.
25. Принципы и условия обработки персональных данных в Российской Федерации.
26. Права субъекта персональных данных в Российской Федерации.
27. Обязанности оператора в Российской Федерации.
28. Государственный контроль и надзор за обработкой персональных данных в Российской Федерации.
29. Ответственность за нарушение законодательства в Российской Федерации в области персональных данных.

**9.6. Контроль освоения компетенций**

| **Вид контроля** | **Контролируемые темы (разделы)** | **Компетенции, компоненты которых контролируются** |
|---|---|---|
| *Устный опрос* | *1,2,3,4* | ПК-1, ПК-2, ПК-3, ПК-6 |

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

| № п/п | Номер и дата протокола заседания кафедры | Перечень измененных пунктов | Подпись заведующего кафедрой |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |