МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ

ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ, ПОЛИТОЛОГИИ И ЗАРУБЕЖНОГО РЕГИОНОВЕДЕНИЯ

Кафедра международной безопасности

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рабочая программа дисциплины

Направление подготовки: 41.04.01 «Зарубежное регионоведение»
Направленность (профиль): «Страны и регионы мира в мировой политике и международном бизнесе»

Квалификация выпускника - магистр
Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Международная информационная безопасность

Рабочая программа дисциплины

Составитель:

кандидат филологических наук, доцент, И.Ю. Бережанская

УТВЕРЖДЕНО

Протокол заседания кафедры международной безопасности

№ 5 от 05.03. 2024

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Дисциплина «Международаня информационная безопасность» является частью профессионального цикла дисциплин подготовки студентов магистратуры по направлению Направление подготовки: 41.04.01 «Зарубежное регионоведение», направленность (профиль): «Страны и регионы мира в мировой политике и бизнесе. »Дислина реализуется на факультете международных отношений, политологии и зарубежного регионоведения ИАИ РГГУ.

Цель дисциплины: формирование у студентов целостных знаний об основах информационной безопасности, средствах массовой информации и их деятельности как в России, так и за рубежом.

Задачи дисциплины:

- ознакомить учащихся с разными видами средств массовой информации;
- выявить особенности работы и политические предпочтения российских и зарубежных (преимущественно западных) СМИ;
- обратить внимание на особенности того, как в отдельных зарубежных СМИ освещается внутренняя и внешняя политика России;
- развить у студентов умение работать с информационными ресурсами, посвященными изучаемой тематике;
- развить навыки полемики с отдельными сюжетами, освещаемыми в СМИ;
- достигнуть творческого осмысления изучаемого материала, на основе полученных знаний, выработка учащимися собственного личностного видения процессов.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция **(код и наименование)**	**Индикаторы компетенций** **(код и наименование)**	**Результаты обучения**
ПК-1 Способен использовать в профессиональной деятельности комплексные знания о регионе специализации с учетом его природных, экономико-географических, исторических, политических, правовых, социальных, экономических, демографических, лингвистических, этнических особенностей.	ПК-1.1. Использует на практике базовые методы регионального анализа, системного регионоведческого описания, и формулирования на его основе практических рекомендаций в интересах профильного министерства, иных государственных или частных организаций, СМИ, информационно-аналитических центров.	Знать: коммуникативные технологии; научные гипотезы и инновационные идеи в области информационной безопасности Уметь: применять различные коммуникативные технологии на иностранном языке; Владеть: навыками выстраивания профессиональной коммуникации на иностранном языке по профилю деятельности. : навыками самостоятельного формулирования научных гипотез и инновационных идей в области информационной безопасности проверки их достоверности.
	ПК-1.2. Готовит экспертно- аналитические материалы (экспертные комментарии,	Знать: базовые принципы анализа угроз международной и информационной безопасности.

	рабочие доклады, аналитические записки) по страноведческой/регионоведческой тематике.	Уметь: выстраивать стратегию подготовки и продвижения докладов, комментариев и публикаций по проблемам информационной безопасности в средствах массовой информации на основе базовых методов и принципов аналитической работы. Владеть: навыками подготовки отчетов и аналитических материалов по проблемам и вопросам информационной безопасности на основе базовых принципов и методов аналитической и экспертной деятельности, современными методами обеспечения защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «*Международная информационная безопасность*» относится к базовой части блока дисциплин учебного плана направление подготовки 41.04.01 «Зарубежное регионоведение», направленности (профиль) «Страны и регионы мира в мировой политике и бизнесе».

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Кросс-региональный анализ», «Интеграционные и дезинтеграционные процессы в регионах мира», «Европейский союз как международный актор», «Внешняя политика США: региональные и глобальные аспекты», прохождения практики по получению первичных профессиональных умений и навыков.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Кибертерроризм в XXI веке как региональная и глобальная угроза», Цифровизация мировой политики и бизнеса», а так же прохождения преддипломной практики.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ак. ч

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	20
3	Семинары	10
Всего:		30

Объем дисциплины в форме самостоятельной работы обучающихся составляет 78 ак.ч,

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Раздел 1. Введение в	Информационная безопасность. Основные

	информационную безопасность	понятия. Модели информационной безопасности. Виды защищаемой информации
2	Раздел 2. Правовое обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны
3	Раздел 3.Организационное обеспечение информационной безопасности	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия
4	Раздел 4. Технические средства и методы защиты информации	Инженерная защита объектов. Защита информации от утечки по техническим каналам
5	Раздел 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз
6	Раздел 6. Криптографические методы защиты информации	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы
7	Раздел 7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности
8	Раздел 8. Использование криптографических средств защиты информации	Создание зашифрованных файлов и криптоконтейнеров и их расшифрование
9	Раздел 9. Реализация работы инфраструктуры открытых ключей	Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи
10	Раздел 10. Средства стеганографии для защиты информации	Использование средств стеганографии для защиты файлов
11	Раздел 11. Настройка безопасного сетевого соединения	Создание защищенного канала связи средствами виртуальной частной сети
12	Раздел 12. Антивирусные средства защиты информации	Изучение настроек средств антивирусной защиты информации

4. Образовательные технологии

Для проведения занятий лекционного типа по дисциплине применяются такие образовательные технологии как интерактивные лекции, проблемное обучение. Для проведения занятий семинарского типа используются групповые дискуссии, анализ ситуаций и решений кейсов.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:
– видео-лекции**;**
– онлайн-лекции в режиме реального времени;
– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
– системы для электронного тестирования;
– консультации с использованием телекоммуникационных средств

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос по вопросам семинаров* *- письменная работа*	 *5 баллов* *30 баллов*	 *30 баллов* *30 баллов*
Промежуточная аттестация *Ответ на контрольные вопросы*	*40 баллов*	*40 баллов*
Итого за семестр *Зачет*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворите льно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Тематика вопросов для опроса

ПК-1 (ПК-1,1; ПК-1.2)

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информа-ции.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информа-ции.
18. Программно-аппаратные средства обеспечения информацион-ной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.

24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Критерии оценки опроса

оценка «неудовлетворительно» (0-2 балла) ставится в том случае, если знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;
оценка «удовлетворительно» (3 балла) выставляется, если материал освоен частично, допущено не более двух-трех недочетов;

оценка «хорошо» (4 балла) выставляется в том случае, если материал освоен почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;

оценка «отлично» (5 баллов) выставляется студенту, если материал освоен полностью, ответ построен по собственному плану.

Баллы суммируются

Максимальное количество – 30 баллов

Темы для письменной работы (реферат)

ПК-1 (ПК-1,1; ПК-1.2)

1. Понятие информационная безопасность.
2. Защита информации, субъект информационных отношений, неприемлемый ущерб.
3. Доступность, целостность, конфиденциальность.
4. Компьютерное преступление, жизненный цикл информационных систем.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Основные понятия программно-технического уровня.
15. Архитектурная безопасность.
16. Анализ защищённости. Отказоустойчивость. Безопасное восстановление.
17. Основные понятия криптографии.
18. Парольная аутентификация.
19. Одноразовые пароли. Сервер аутентификации
20. Идентификация/аутентификация с помощью биометрических данных.
21. Ролевое управление доступом.
22. Активный аудит. Шифрование.
23. Секретный и открытый ключ.
24. Криптография. Контроль целостности

Критерии оценки письменной работы (реферат)

оценка «отлично» (30-25 баллов) выставляется студенту, если он дал исчерпывающие ответы на задания; ответы хорошо и логично структурированы, написаны хорошим научным языком, грамотно;

оценка «хорошо» (24-16) баллов) выставляется в том случае, если даны довольно полные ответы на задания, но допущены неточности, есть отдельные ошибки; нарушена структура ответа;

оценка «удовлетворительно» (15-19 баллов) ставится, если ответы на задания неполные, есть ошибки; написано небрежно, нет хорошей структуры ответа;

оценка «неудовлетворительно» (0-9) баллов) ставится в том случае, если либо фактически не выполнены задания, либо нет демонстрации общей эрудиции и знаний лекционного материала.

Максимум – 30 баллов

Контрольные вопросы для аттестации)

ПК-1 (ПК-1,1; ПК-1.2)

1.Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.

2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.

3. Сложные системы. Структурный подход.

4. Основные определения и критерии классификации угроз.

5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.

6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.

7. Российское законодательство в области информационной безопасности.

8. Зарубежное законодательство в области информационной безопасности.

9. Стандарты и спецификации в области информационной безопасности.

10. Основные понятия, политика безопасности.

11. Жизненный цикл информационной системы.

12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.

13. Основные классы мер процедурного уровня.

14. Управление персоналом. Физическая защита.

15. Поддержание работоспособности.

16. Реагирование на нарушения режима безопасности.

17. Планирование восстановительных работ.

18. Основные понятия программно-технического уровня. Архитектурная безопасность.

19. Экранирование. Анализ защищённости.

20. Отказоустойчивость. Безопасное восстановление.

21. Основные понятия криптографии.

22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации

23. Kerberos.

24. Идентификация/аутентификация с помощью биометрических данных.

25. Управление доступом. Ролевое управление доступом.

26. Активный аудит. Шифрование.

27. Симметричный метод шифрования.

28. Асимметричный метод шифрования.

29. Секретный и открытый ключ.

30. Криптография. Контроль целостности

Критерии оценки

При проведении промежуточной аттестации в виде зачета с оценкой (экзамена) студент должен ответить на 2 вопроса. При оценивании ответа на вопрос учитывается:

оценка «неудовлетворительно» (0-9 баллов) ставится в том случае, если знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;

оценка «удовлетворительно» (20-10 баллов) выставляется, если материал освоен частично, допущено не более двух-трех недочетов;

оценка «хорошо» (30-21 баллов) выставляется в том случае, если материал освоен почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;

оценка «отлично» (40-31 баллов) выставляется студенту, если материал освоен полностью, ответ построен по собственному плану.

Максимум - 40 баллов

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основные источники

Конституция Российской Федерации.

Уголовный кодекс Российской Федерации.

Федеральный закон № 149-ФЗ от 27.07.2006 (включая изменения и дополнения) «Об информации, информационных технологиях и защите информации».

Федеральный закон № 125-ФЗ от 22.10.2004 (включая изменения и дополнения) «Об архивном деле в Российской Федерации».

Федеральный закон № 128-ФЗ от 8.08.2001 «О лицензировании отдельных видов деятельности».

Федеральный закон № 152-ФЗ от 27.07.2006 (включая изменения и дополнения) «О персональных данных».

Федеральный закон № 85-ФЗ от 4.07.1996 «Об участии в международном информационном обмене».

Основная литература

Учебная

1. Бартош, А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А. А. Бартош. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 429 с. — (Высшее образование). — ISBN 978-5-534-17521-9. — URL : https://urait.ru/bcode/540122
2. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 57 с. — (Высшее образование). — ISBN 978-5-534-17204-1. — URL : https://urait.ru/bcode/544885
3. Гетьман-Павлова, И. В. Международное право : учебник для вузов / И. В. Гетьман-Павлова, Е. В. Постникова. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 590 с. — (Высшее образование). — ISBN 978-5-534-18831-8. — URL : https://urait.ru/bcode/551768
4. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — URL : https://urait.ru/bcode/544290
5. Нестеров, С. А. Информационная безопасность / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — URL : https://urait.ru/bcode/434171

6. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — URL : https://urait.ru/bcode/449350
7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — URL : https://urait.ru/bcode/536225
8. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — URL : https://urait.ru/bcode/543351
9. Кисляков, П. А. Безопасность образовательной среды. Социальная безопасность : учебное пособие для вузов / П. А. Кисляков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 156 с. — (Высшее образование). — ISBN 978-5-534-11818-6. — URL : https://urait.ru/bcode/456941
10. Трофимов, В. В. Глобальные и локальные сети : учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 162 с. — (Высшее образование). — ISBN 978-5-534-17504-2. — URL : https://urait.ru/bcode/545060

Дополнительная литература

1. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Издательство Юрайт, 2024. — 301 с. — (Актуальные монографии). — ISBN 978-5-534-14919-7. — URL : https://urait.ru/bcode/544238
2. 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. — URL : https://urait.ru/bcode/545066
3. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 347 с. — (Высшее образование). — ISBN 978-5-534-04348-8. — URL : https://urait.ru/bcode/449839
4. Информационные технологии в юридической деятельности В. Д. Элькин [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 403 с. — (Высшее образование). — ISBN 978-5-9916-5283-4. — URL : https://urait.ru/bcode/431764
5. Информационные технологии в юридической деятельности : учебник для вузов / П. У. Кузнецов [и др.] ; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — URL : https://urait.ru/bcode/449842
6. Плахотникова, М. А. Информационные технологии в менеджменте / М. А. Плахотникова, Ю. В. Вертакова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 326 с. — (Профессиональное образование). — ISBN 978-5-534-09488-6. — URL : https://urait.ru/bcode/452349
7. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт,

2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — URL : https://urait.ru/bcode/449285
8. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : https://urait.ru/bcode/450820
9. Кузнецова, Е. И. Экономическая безопасность : учебник и практикум для вузов / Е. И. Кузнецова. — Москва : Издательство Юрайт, 2020. — 294 с. — (Высшее образование). — ISBN 978-5-534-09032-1. — URL : https://urait.ru/bcode/451954
10. Экономическая информатика : учебник и практикум для бакалавриата и магистратуры / Ю. Д. Романова [и др.] ; ответственный редактор Ю. Д. Романова. — Москва : Издательство Юрайт, 2019. — 495 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-9916-3770-1. — URL : https://urait.ru/bcode/426110
11. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Издательство Юрайт, 2020. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. — URL : https://urait.ru/bcode/448300

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases
Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины используются: компьютерный класс с возможностью презентации в системе «Power Point» с лицензионным программным обеспечением с доступом в Интернет.

1. Windows
2. Microsoft Office
3. Adobe Master Collection
4. AutoCAD
5. Archicad
6. SPSS Statisctics
7. ОС «Альт Образование»
8. Visual Studio
9. Adobe Creative Cloud

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:
для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

для глухих и слабослышащих:
- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

для лиц с нарушениями опорно-двигательного аппарата:
- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для слепых и слабовидящих:
- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

для глухих и слабослышащих:
- в печатной форме;
- в форме электронного документа.

для обучающихся с нарушениями опорно-двигательного аппарата:
- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:
- устройством для сканирования и чтения с камерой SARA CE;

- дисплеем Брайля PAC Mate 20;
- принтером Брайля EmBraille ViewPlus;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы семинарских занятий

Семинарское занятие № 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности – 2 ч.

Обсуждаемые вопросы:

Перечислите основные угрозы информационной безопасности.

Какие существуют модели информационной безопасности?

Какие методы защиты информации выделяют?

Что такое правовые методы защиты информации?

Что такое организационные методы защиты информации?

Семинарское занятие № 2. Использование криптографических средств защиты информации- 1 ч..

Обсуждаемые вопросы:

Что такое технические методы защиты информации?

Что такое программно-аппаратные методы защиты информации?

Что такое криптографические методы защиты информации?

Что такое физические методы защиты информации?

Обязательные источники и литература:

Конституция Российской Федерации.

Семинарское занятие № 3. Реализация работы инфраструктуры открытых ключей- 1 ч.

Обсуждаемые вопросы:

Что такое цифровая подпись?

Что такое инфраструктура открытых ключей?

Какие российские и международные стандарты на формирование цифровой подписи существуют?

Семинарское занятие № 4. Средства стеганографии для защиты информации – 2 ч..

Обсуждаемые вопросы:

Что такое механизм контроля и разграничения доступа?

Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?

Что такое средства стеганографической защиты информации?

Семинарское занятие № 5. Настройка безопасного сетевого соединения. – 1ч.

Обсуждаемые вопросы:

Перечислите методы защиты информации от утечки по индук-ционному каналу.

Перечислите средства и методы защиты информации от утечки в телефонных линиях.

Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Семинарское занятие № 6. Антивирусные средства защиты информации.- 1 ч.

Обсуждаемые вопросы:

Какие виды компьютерных угроз существуют?

Что такое брандмауэр?

Что такое антивирусная программа?

Что такое эвристический алгоритм поиска вирусов?

Что такое сигнатурный поиск вирусов?

Методы противодействия сниффингу?

Какие программные реализации программно-аппаратных средств защиты информации вы знаете?

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Международная информационная безопасность» относится к базовой части блока дисциплин учебного плана направление подготовки 41.04.01 «Зарубежное регионоведение», направленности (профиль) «Страны и регионы мира в мировой политике и бизнесе». Дисциплина реализуется на факультете международных отношений, политологии и зарубежного регионоведения ИАИ РГГУ.

Цель дисциплины: формирование у студентов целостных знаний об основах информационной безопасности, средствах массовой информации и их деятельности как в России, так и за рубежом.

Задачи дисциплины: ознакомить учащихся с разными видами средств массовой информации;

- выявить особенности работы и политические предпочтения российских и зарубежных (преимущественно западных) СМИ;
- обратить внимание на особенности того, как в отдельных зарубежных СМИ освещается внутренняя и внешняя политика России;
- развить у студентов умение работать с информационными ресурсами, посвященными изучаемой тематике;
- развить навыки полемики с отдельными сюжетами, освещаемыми в СМИ;
- достигнуть творческого осмысления изучаемого материала, на основе полученных знаний, выработка учащимися собственного личностного видения процессов.

В результате освоения дисциплины обучающийся должен продемонстрировать следующие результаты образования:

Знать: базовые принципы анализа угроз международной безопасности, современные законы, стандарты, методы и технологии в области защиты информации; требования к защите информации определенного типа.

Уметь: применять различные коммуникативные технологии на иностранном языке; выстраивать стратегию подготовки и продвижения докладов, комментариев и публикаций по проблемам информационной безопасности в средствах массовой информации на основе базовых методов и принципов аналитической работы; использовать современные программно-аппаратные средства защиты информации; подобрать и обеспечить защиту информации.

Владеть: навыками выстраивания профессиональной коммуникации на иностранном языке по профилю деятельности. навыками самостоятельного формулирования научных гипотез и инновационных идей в области информационной безопасности проверки их достоверности, навыками подготовки отчетов и аналитических материалов по проблема и вопросам международной безопасности на основе базовых принципов и методов аналитической и экспертной деятельности, современными методами обеспечения защиты информации.