

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
"Казанский (Приволжский) федеральный университет"  
Институт международных отношений  
Отделение Высшая школа международных отношений и востоковедения



УТВЕРЖДАЮ  
Проректор по образовательной деятельности КФУ  
проф. Таюрский Д.А.  
"\_\_\_" 20\_\_ г.

## Программа дисциплины

Информационно-психологическая кибербезопасность Б1.В.01.01

Направление подготовки: 41.04.05 - Международные отношения

Профиль подготовки: Цифровая дипломатия

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2018

Автор(ы): Ахметкаимов Б.Г., Саляхутдинова Елена Владимировна

Рецензент(ы): Летяев В.А.

### СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Летяев В. А.

Протокол заседания кафедры № \_\_\_\_ от "\_\_\_\_" 20\_\_ г.

Учебно-методическая комиссия Института международных отношений (отделение Высшая школа международных отношений и востоковедения):

Протокол заседания УМК № \_\_\_\_ от "\_\_\_\_" 20\_\_ г.

## **Содержание**

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
  - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
  - 4.2. Содержание дисциплины
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
  - 6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения
  - 6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания
  - 6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы
  - 6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)
  - 7.1. Основная литература
  - 7.2. Дополнительная литература
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Программу дисциплины разработал(а)(и) доцент, к.н. Ахметкаимов Б.Г. (Кафедра международных отношений, мировой политики и дипломатии, отделение Высшая школа международных отношений и востоковедения), BGAhmetkarimov@kpfu.ru ; Салихутдинова Елена Владимировна

**1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы**

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1 (ЭА)	

Выпускник, освоивший дисциплину:

Должен демонстрировать способность и готовность:

Обучающийся должен демонстрировать способность и готовность объяснить, что имеется в виду под киберпространством и кибербезопасностью; обозначить некоторые основные уязвимости развитых государств перед киберугрозами; описать основную топологию киберпространства, включая его физические структуры, а также то, как оно управляетя протоколами и процедурами; и сформулировать основные принципы надлежащей архитектуры безопасности.

**2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования**

Данная учебная дисциплина включена в раздел "Б1.В.01.01 Дисциплины (модули)" основной профессиональной образовательной программы 41.04.05 "Международные отношения (Цифровая дипломатия)" и относится к вариативной части.

Осваивается на 1 курсе в 2 семестре.

**3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 36 часа(ов), в том числе лекции - 10 часа(ов), практические занятия - 26 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 72 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен во 2 семестре.

**4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)**

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Киберпространство и основы кибербезопасности	2	2	6	0	20
2.	Тема 2. Информационная безопасность и риски	2	3	6	0	20
3.	Тема 3. Международные организации по кибербезопасности, принципы и стандарты	2	3	6	0	15
4.	Тема 4. Менеджмент кибербезопасности в национальном контексте	2	2	8	0	17

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
	Итого		10	26	0	72

#### 4.2 Содержание дисциплины

##### **Тема 1. Киберпространство и основы кибербезопасности**

Кибербезопасность и киберпространство - введение

Структура информационного пространства: опорная сеть Интернета и сетевая инфраструктура государств

Архитектура сетевой безопасности и управление процессом обеспечения безопасности

Общие сведения о безопасности ПК и Интернета

Техника безопасности и экология

Проблемы Интернет-зависимости

Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы

Мошеннические действия в Интернете. Киберпреступления

##### **Тема 2. Информационная безопасность и риски**

Риск, связанный с мобильностью, личные мобильные устройства и новые тенденции

Нападения из удаленного доступа.

Здоровый образ жизни и компьютер. Виды зависимости. Как определить наличие зависимости

Как распространяются вирусы

Утечка и обнародование личных данных

Подмена сайтов в интернете (сайты-клоны).

Фальшивые файлообменники

##### **Тема 3. Международные организации по кибербезопасности, принципы и стандарты**

Международные стандарты и требования: обзор структур и практических действий

Кибербезопасность в международном законодательстве

Международный стандарт ISO/IEC 27032

Информационные технологии. Методы обеспечения безопасности.

Руководящие указания по кибербезопасности

безопасность онлайновых операций, обмена персональной информацией через Интернет

##### **Тема 4. Менеджмент кибербезопасности в национальном контексте**

Национальные методы работы, принципы действия и организации по киберустойчивости

Национальные структуры кибербезопасности

Киберкриминалистика

Аудит и оценка безопасности на национальном уровне

ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект Концепции стратегии кибербезопасности Российской Федерации

Анализ международного стандарта ISO/IEC 27032.

#### **5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)**

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301).

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Положение от 24 декабря 2015 г. № 0.1.1.67-06/265/15 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет""

Журнал "Вопросы кибербезопасности" - <http://cyberrus.com/>

Инженерный совет Интернета (IETF) - <https://www.ietf.org/standards/rfcs/>

Кибер Россия - федеральная образовательная программа - [cyber-russia.ru/](http://cyber-russia.ru/)

## 6. Фонд оценочных средств по дисциплине (модулю)

### 6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
<b>Семестр 2</b>			
	<b>Текущий контроль</b>		
1	Реферат	ПК-1 (ЭА)	1. Киберпространство и основы кибербезопасности 2. Информационная безопасность и риски 3. Международные организации по кибербезопасности, принципы и стандарты 4. Менеджмент кибербезопасности в национальном контексте
2	Презентация	ПК-1 (ЭА)	1. Киберпространство и основы кибербезопасности 2. Информационная безопасность и риски 3. Международные организации по кибербезопасности, принципы и стандарты 4. Менеджмент кибербезопасности в национальном контексте
3	Дискуссия	ПК-1 (ЭА)	2. Информационная безопасность и риски
	<b>Экзамен</b>		

### 6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап	
	Отлично	Хорошо	Удовл.	Неуд.		
<b>Семестр 2</b>						
<b>Текущий контроль</b>						

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Реферат	Тема раскрыта полностью. Продемонстрировано превосходное владение материалом. Использованы надлежащие источники в нужном количестве. Структура работы соответствует поставленным задачам. Степень самостоятельности работы высокая.	Тема в основном раскрыта. Продемонстрировано хорошее владение материалом. Использованы надлежащие источники. Структура работы в основном соответствует поставленным задачам. Степень самостоятельности работы средняя.	Тема раскрыта слабо. Продемонстрировано удовлетворительное владение материалом. Использованные источники и структура работы частично соответствуют поставленным задачам. Степень самостоятельности работы низкая.	Тема не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны. Структура работы не соответствует поставленным задачам. Работа несамостоятельна.	1
Презентация	Превосходный уровень владения материалом. Высокий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения полностью соответствуют задачам презентации. Использованы надлежащие источники и методы.	Хороший уровень владения материалом. Средний уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения в основном соответствуют задачам презентации. Использованные источники и методы в основном соответствуют поставленным задачам.	Удовлетворительный уровень владения материалом. Низкий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения слабо соответствуют задачам презентации. Использованные источники и методы частично соответствуют поставленным задачам.	Неудовлетворительный уровень владения материалом. Неудовлетворительный уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения не соответствуют задачам презентации. Использованные источники и методы не соответствуют поставленным задачам.	2
Дискуссия	Высокий уровень владения материалом по теме дискуссии. Превосходное умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Высокий уровень этики ведения дискуссии.	Средний уровень владения материалом по теме дискуссии. Хорошее умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Средний уровень этики ведения дискуссии.	Низкий уровень владения материалом по теме дискуссии. Слабое умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Низкий уровень этики ведения дискуссии.	Недостаточный уровень владения материалом по теме дискуссии. Неумение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Отсутствие этики ведения дискуссии.	3

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.	

### 6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

#### Семестр 2

##### Текущий контроль

###### 1. Реферат

Темы 1, 2, 3, 4

1. Урегулирование киберрисков в контексте национальной политики
2. Государственные органы и структуры, играющие ведущую роль в обеспечении информационной безопасности в компьютерных системах
3. стандарты безопасности в сфере информационных и электронных систем
4. Ключевые проблемы в области информационно-коммуникационных технологий
5. Что такое аудит информационной безопасности?
6. Что считается несанкционированным доступом к информации предприятия?
7. Как нарушается информационная безопасность техническими способами воздействия?
8. Какие существуют виды возможных угроз в информационной среде?
9. Методы защиты информации
10. Методы оценки рисков информационной безопасности

###### 2. Презентация

Темы 1, 2, 3, 4

1. Актуальные виды угроз информационной безопасности
2. Государственные органы и структуры, играющие ведущую роль в обеспечении информационной безопасности в компьютерных системах
3. стандарты безопасности в сфере информационных и электронных систем
4. Ключевые проблемы в области информационно-коммуникационных технологий
5. Что такое аудит информационной безопасности?
6. Что считается несанкционированным доступом к информации предприятия?
7. Как нарушается информационная безопасность техническими способами воздействия?
8. Какие существуют виды возможных угроз в информационной среде?
9. Методы защиты информации

## 10. Методы оценки рисков информационной безопасности

### 3. Дискуссия

#### Тема 2

1. Риск, связанный с мобильностью
2. личные мобильные устройства и новые тенденции
3. Нападения из удаленного доступа.
4. Здоровый образ жизни и компьютер. Виды зависимости. Как определить наличие зависимости
5. Как распространяются вирусы
6. Утечка и обнародование личных данных

### Экзамен

Вопросы к экзамену:

1. Эволюция информационной безопасности
2. Государственные органы и структуры, играющие ведущую роль в обеспечении информационной безопасности в компьютерных системах
3. стандарты классификации безопасности в сфере информации, а также информационных и электронных систем
4. Ключевые проблемы в области информационно-коммуникационных технологий
5. Что такое аудит информационной безопасности?
6. Что считается несанкционированным доступом к информации предприятия?
7. Как нарушается информационная безопасность техническими способами воздействия?
8. Какие существуют виды возможных угроз в информационной среде?
9. Методы защиты информации
10. Методы оценки рисков информационной безопасности

### 6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

- 56 баллов и более - "зачтено".  
55 баллов и менее - "не зачтено".

Для экзамена:

- 86 баллов и более - "отлично".  
71-85 баллов - "хорошо".  
56-70 баллов - "удовлетворительно".  
55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
<b>Семестр 2</b>			
<b>Текущий контроль</b>			
Реферат	Обучающиеся самостоятельно пишут работу на заданную тему и сдают преподавателю в письменном виде. В работе производится обзор материала в определённой тематической области либо предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения. В случае публичной защиты реферата оцениваются также ораторские способности.	1	20
Презентация	Обучающиеся выполняют презентацию с применением необходимых программных средств, решая в презентации поставленные преподавателем задачи. Обучающийся выступает с презентацией на занятии или сдаёт её в электронном виде преподавателю. Оцениваются владение материалом по теме презентации, логичность, информативность, способы представления информации, решение поставленных задач.	2	20

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Дискуссия	На занятии преподаватель формулирует проблему, не имеющую однозначного решения. Обучающиеся предлагают решения, формулируют свою позицию, задают друг другу вопросы, выдвигают аргументы и контраргументы в режиме дискуссии. Оцениваются владение материалом, способность генерировать свои идеи и давать обоснованную оценку чужим идеям, задавать вопросы и отвечать на вопросы, работать в группе, придерживаться этики ведения дискуссии.	3	10
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

## 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

### 7.1 Основная литература:

1. Основы борьбы с киберпреступностью и кибертерроризмом [Электронный ресурс] : хрестоматия / сост. В. С. Овчинский. ? М. : Норма, 2017. ? 528 с. Режим доступа:

<http://znanium.com/catalog/product/771246>

2. Международные отношения: теории, конфликты, движения, организации [Электронный ресурс] : Учебное пособие / П.А. Цыганков, Г.А. Дробот, А.И. Слива и др. - 3-е изд., перераб. и доп. - М.: Альфа-М: ИНФРА-М, 2011. - 336 с.: 60x90 1/16. (п) ISBN 978-5-98281-212-4 - Режим доступа: <http://znanium.com/catalog/product/246855>

3. Международные отношения: традиции русской политической мысли [Электронный ресурс] : Учебное пособие / А.П. Цыганков. - М.: Альфа-М: НИЦ ИНФРА-М, 2013. - 336 с.: ил.; 60x90 1/16. ISBN 978-5-98281-325-1 - Режим доступа: <http://znanium.com/catalog/product/368959>

### 7.2. Дополнительная литература:

1. Правовое регулирование в сфере информационных технологий [Электронный ресурс] : Учебное пособие / Епифанов С.С. - Рязань:Академия ФСИН России, 2012. - 73 с.: ISBN 978-5-7743-0535-3 - Режим доступа: <http://znanium.com/catalog/product/774204>

2. Психология [Электронный ресурс] / Караванова Л.Ж. - М.:Дашков и К, 2017. - 264 с.: ISBN 978-5-394-02247-0 - Режим доступа: <http://znanium.com/catalog/product/450768>

3. Современные информационные технологии для гуманитария [Электронный ресурс] : Практическое руководство / А.Т. Хроленко, А.В. Денисов. - М.: Флинта: Наука, 2007. - 128 с.: 60x88 1/16. (e-book) ISBN 978-5-9765-0023-5 Режим доступа: <http://znanium.com/catalog/product/320764>

## 8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Skoltech - <https://www.skoltech.ru/en>

Кибер Россия - [kiberrossiya.ru/education](http://kiberrossiya.ru/education)

Центр Кибербезопасности НИЯУ МИФИ - [cc.mephi.ru/](http://cc.mephi.ru/)

## 9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	На лекционном занятии преподаватель формулирует проблему, не имеющую однозначного решения. Обучающиеся предлагают решения, формулируют свою позицию, задают друг другу вопросы, выдвигают аргументы и контраргументы в режиме дискуссии. Оцениваются владение материалом, способность генерировать свои идеи и давать обоснованную оценку чужим идеям, задавать вопросы и отвечать на вопросы, работать в группе, придерживаться этики ведения дискуссии. Методика подготовки к дискуссии предполагает уяснение плана дискуссии и ознакомление с контекстом и проблематикой, подготовку устного выступления сроком не более 5 минут, ознакомление с терминологией, подбор аргументов в защиту избранной позиции. При работе с терминами необходимо обращаться к словарям, в том числе доступным в Интернете, например на сайте <a href="http://dic.academic.ru">http://dic.academic.ru</a> .

Вид работ	Методические рекомендации
практические занятия	<p>Практические занятия помогают студентам глубже усвоить учебный материал, приобрести навыки творческой работы над дипломатическими документами и другими первоисточниками. Планы семинарских занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях или в методических указаниях по данной дисциплине. Прежде чем приступить к изучению темы, необходимо прокомментировать основные вопросы плана семинара. Такой подход преподавателя помогает студентам быстро находить нужный материал к каждому из вопросов, не задерживаясь на второстепенном. Начиная подготовку к семинарскому занятию, необходимо, прежде всего, указать студентам разделы учебников и учебных пособий, материалы на профильных сайтах, чтобы они получили общее представление о месте и значении темы в изучаемом курсе. Затем следует рекомендовать им поработать с дополнительной литературой, сделать записи по рекомендованным источникам.♦</p>
самостоятельная работа	<p>Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно дома и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий. Выполнение письменных заданий нужно начинать с повторения теоретического материала, то есть с работы над учебником. Письменная домашняя работа выполняется с делением её на части в соответствии со структурой задания. Ответ по каждому пункту должен включать 1) формулировку проблемы; 2) анализ свойств конкретной ситуации с применением для решения поставленных целей и задач. Письменное домашнее задание должно содержать: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме. Алгоритм работы может быть следующим: определение, осмысление и соотнесение с темой эссе собственной позиции по каждой из рассматриваемых точек зрения; аргументированное оформление своей позиции в отношении каждой из анализируемых точек зрения в форме тезисов: выбор эффектной цитаты, точной мысли, интересного факта, убедительного аргумента. Мысль должна быть подкреплена доказательствами, поэтому за тезисом следуют аргументы. Аргументация своей позиции должна опираться на факты общественной жизни, мнения специалистов, а не сводится к простому описанию на основе непроверенных источников информации.♦</p>
презентация	<p>Обучающиеся выполняют презентацию с применением необходимых программных средств, решая в презентации поставленные преподавателем задачи. Обучающийся выступает с презентацией на занятии или сдаёт её в электронном виде преподавателю. Оцениваются владение материалом по теме презентации, логичность, информативность, способы представления информации, решение поставленных задач.♦</p>
реферат	<p>Обучающиеся самостоятельно пишут работу на заданную тему и сдают преподавателю в письменном виде. В работе производится обзор материала в определённой тематической области либо предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения. В случае публичной защиты реферата оцениваются также ораторские способности.</p>
дискуссия	<p>На занятии преподаватель формулирует проблему, не имеющую однозначного решения. Обучающиеся предлагают решения, формулируют свою позицию, задают друг другу вопросы, выдвигают аргументы и контраргументы в режиме дискуссии. Оцениваются владение материалом, способность генерировать свои идеи и давать обоснованную оценку чужим идеям, задавать вопросы и отвечать на вопросы, работать в группе, придерживаться этики ведения дискуссии.</p>
экзамен	<p>Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.</p>

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

Освоение дисциплины "Информационно-психологическая кибербезопасность" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Браузер Google Chrome

Adobe Reader XI

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

## **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Освоение дисциплины "Информационно-психологическая кибербезопасность" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

## **12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья**

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи;
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 41.04.05 "Международные отношения" и магистерской программе Цифровая дипломатия .