

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет психологии и философии

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Кафедра философии и социально-политических наук

Факультет психологии и философии

Направление: 41.03.04 - Политология

Направленность (профиль) программы:
Общий

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины:
Дисциплина по выбору

Махачкала, 2021

Рабочая программа дисциплины «Информационная безопасность» составлена в 2021 году в соответствии с требованиями ФГОС ВО по направлению подготовки 41.03.04 Политология, уровень бакалавриата от 23 августа 2017 г. № 814.

Разработчик:

Кафедра философии и социально-политических наук, кандидат философских наук, доцент



Алибекова С.Я.

Рабочая программа дисциплины одобрена:

на заседании кафедры философии и социально-политических наук от «09» 06 2021 г., протокол № 9

Зав. кафедрой



Яхьяев М.Я.

на заседании Методической комиссии факультета психологии и философии от «02» 07 2021 г., протокол № 4

Председатель

Билалов М.И.



Рабочая программа дисциплины согласована с учебно-методическим управлением от «09» 07 2021 г.

Начальник УМУ



Гасангаджиева А. Г.

Аннотация рабочей программы дисциплины

Дисциплина «Информационная безопасность» входит в основную профессиональную образовательную программу бакалавриата по направлению подготовки 41.03.04 Политология, профиль подготовки общий, как дисциплина по выбору.

Дисциплина реализуется на факультете психологии и философии кафедрой философии и социально-политических наук.

Содержание дисциплины охватывает круг вопросов, связанных с переходом к новому типу социальной организации общества, имеющему информационную и сетевую природу - открытому информационному обществу. Глубокой трансформацией охвачены основные сферы жизнедеятельности социума: взаимодействие с природой; общественные отношения; политическая регуляция. Производство материальных благ, создание культурных ценностей и осуществление власти становятся напрямую зависимыми от технологических возможностей общества, основу которых составляют информационные и коммуникационные технологии.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных: ОПК-1; ОПК-2; профессиональных: ПК-4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа..

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме контроля текущей успеваемости: устный опрос, коллоквиум, контрольная работа и промежуточный контроль в форме зачета.

Объем дисциплины: 2 зачетных единиц, в том числе в академических часах по видам учебных занятий.

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:							
	всего	Контактная работа обучающихся с преподавателем			из них		СРС, в том числе экзамен	
		всего	Лекции	Лабораторные занятия	Практические занятия	КСР		
3	72	36	18		18		36	зачет

1.Цели освоения дисциплины

Целями освоения дисциплины (модуля) являются: приобретение студентами необходимых знаний и навыков об информационной политике как о закономерно развивающейся системе в условиях построения демократической государственности и формирования информационного общества на основе использования информационных и телекоммуникационных технологий;

ознакомление студентов с особенностями информационно-коммуникационных процессов разного уровня, а также специфики проведения информационных кампаний.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность» входит в основную профессиональную образовательную программу бакалавриата по направлению подготовки 41.03.04 Политология, профиль подготовки общий, как дисциплина по выбору.

В процессе изучения материала студенты должны усвоить теоретические, методологические, методические и прикладные основы информационной политики в их единстве. Это позволит понять междисциплинарный характер этой дисциплины, современную проблематику и технологию решения задач в сфере политико-коммуникационной деятельности, способы организации и проведения научных исследований и разработок. А также позволит самостоятельно находить пути и способы повышения эффективности информационно-коммуникационных систем и технологий, их нацеленность на решение стратегических и оперативных задач современной политической жизни и в системе государственно-властного управления различного уровня.

Курс входит в число общепрофессиональных дисциплин, формирующих подготовку бакалавра в области политологии. Он тесно связан с общими политологическими дисциплинами. В методическом плане дисциплина опирается на знания, полученные при изучении следующих учебных курсов: «Политическая социология», «Теория политики», «Политическая психология».

Курс служит основой для продолжения изучения различных аспектов политического бытия и углубления базовых представлений о методическом обеспечении исследовательского процесса. Освоение материала значительно повышает способности студентов к самостоятельной творческой работе и их готовность к аналитическим заключениям.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения и процедура освоения).

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенций (в соответствии с ОПОП)	Планируемые результаты обучения	Процедура освоения
ОПК-1 ОПК-1. Спо-собен осуществлять эффективную коммуникацию в мультикультурной профессиональной среде на государственном языке Российской Федерации и иностран-	ОПК-1.1. Спо-собен осуществлять эффективную коммуникацию в мультикультурной профессиональной среде на государственном языке Российской Федерации. на основе применения понятийного аппарата по профилю де-	Знает: -понятий-ный аппарат по профилю деятельности; - мульти-культурную профессиональную среду - средства эффективной межкультурной коммуникации в том числе в публичном пространстве на государственном языке Российской Федерации, с учетом особенностей мультикультурной среды. Философия, Иностранный язык, Русский язык и культура речи, Деловая коммуникация в профессио-	Устный опрос, письменный опрос; лекция-дискуссия, лекция-беседа;

<p>ном(ых) языке(ах) на основе применения понятийного аппарата по профилю деятельности</p>	<p>тельности</p>	<p>нальной деятельности, Иностранный язык в профессиональной деятельности, Основы менеджмента и PR в сфере публичного управления, Политическая риторика, Риторика: ключевые стратегии устной и письменной коммуникации, Информационная политика, Информационная безопасность, Телекоммуникационные и компьютерные</p> <p>- знает этические и культурные нормы коммуникации в публичном и информационном пространстве, в том числе с применением цифровых и информационных технологий.. Умеет: - применять понятийный аппарат по профилю деятельности на государственном языке Российской Федерации; - использовать основные стратегии, тактические приемы и технологии в PR, Информационные технологии и программирование в политике, Учебная практика, ознакомительная, Научно-исследовательская работа (по теме выпускной квалификационной работы), Производственная практика: преддипломная практика.</p> <p>емы и техники аргументации с целью последовательного выстраивания позиции представляемой стороны в мультикультурной профессиональной среде - применять эффективные переговорные технологии в</p>	
--	------------------	--	--

		<p>межкультурной коммуникации в том числе в публичном пространстве на государственном языке Российской Федерации. - применять этические и культурные нормы коммуникации, в публичном и информационном пространстве, в дипломатии и деловом общении, в том числе с применением цифровых и информационных технологий.</p> <p>Владеет: - навыками оперирования понятийным аппаратом по профилю деятельности на государственном языке Российской Федерации; - навыками и приемами техники аргументации с целью последовательного выстраивания позиции представляемой стороны в мультикультурной профессиональной среде - вести эффективные переговоры в межкультурной коммуникации в том числе в публичном пространстве на государственном языке Российской Федерации. - навыками этических и культурных норм коммуникаций, в публичном и информационном пространстве, в дипломатии и деловом общении, в том числе с применением цифровых и информационных технологий</p>	
	<p>ОПК 1.2. Способен осуществлять эф-</p>	<p>Знает: -понятийный аппарат по профилю деятельности; - мультикультур-</p>	

	<p>фективную коммуникацию в мультикультурной профессиональной среде на иностранном(ых) языке(ах) на основе применения понятийного аппарата по профилю деятельности</p>	<p>ную профессиональную среду - средства эффективной межкультурности турной коммуникации в том числе в публичном пространстве на иностранном(ых) языке(ах), с учетом особенностей мультикультурной среды. - знает этические и культурные нормы коммуникации в публичном и информационном пространстве, в том числе с применением цифровых и информационных технологий на иностранном(ых) языке(ах).. Умеет: - применять понятийный аппарат по профилю деятельности на иностранном(ых) языке(ах); - использовать основные стратегии, тактические приемы и техники аргументации с целью последовательного выстраивания позиции представляемой стороны в мультикультурной профессиональной среде - применять эффективные переговорные технологии в межкультурной коммуникации в том числе в публичном пространстве на иностранном(ых) языке(ах). - применять этические и культурные нормы коммуникации, в публичном и информационном пространстве, в дипломатии и деловом общении, в том числе с применением цифровых и информационных технологий</p>	
--	--	--	--

		<p>на иностранном(ых) языке(ах). Владеет: - навыками оперирования понятийным аппаратом по профилю деятельности на иностранном(ых) языке(ах); - навыками и приемами техники аргументации с целью последовательного выстраивания позиции представляемой стороны в мультикультурной профессиональной среде на иностранном(ых) языке(ах) - вести эффективные переговоры в межкультурной коммуникации в том числе в публичном пространстве на иностранном(ых) языке(ах). - навыками этических и культурных норм коммуникаций, в публичном и информационном пространстве, в дипломатии и деловом общении, в том числе с применением цифровых и информационных технологий на иностранном(ых) языке(ах).</p>	
...	
...	презентации
ОПК-2. Способен применять информационно-коммуникационные технологии и программные средства для решения стандартных задач профессиона-	ОПК-2.1. Способен применять информационно-коммуникационные технологии и программные средства для решения стандартных задач профессиона-	Знает: - приемы и методы информационной коммуникации и программные средства для решения стандартных задач профессиональной деятельности на основе информационной культуры и требований информационной безопасности Умеет: Введение в информаци-	Письменный опрос написание эссе

<p>нальной деятельности на основе информационной и библиографической культуры и требований информационной безопасности</p>	<p>нальной деятельности на основе информационной культуры и требований информационной безопасности</p>	<p>онные технологии, Статистика, Методы комплексных исследований в сфере политических наук и регионоведения, Информационная политика, Информационная безопасность, Телекоммуникационные и компьютерные технологии в PR Информационные технологии и программирование в политике, Учебная практика, ознакомительная, Научно-исследовательская работа (по теме</p> <p>- применять приемы и методы информационной коммуникации и и программные средства для решения стандартных задач профессиональной деятельности на основе информационной культуры и требований информационной безопасности. Владеет: - навыками информационной коммуникации и и программно-выпускной квалификационной работы) Производственная практика: преддипломная практика средствами для решения стандартных задач профессиональной деятельности на основе информационной культуры и требований информационной безопасности.</p>	
	<p>ОПК-2.2. Способен применять информационно-</p>	<p>Знает: - приемы и методы информационной коммуникации и и программные средства для решения стандартных задач профессиональной</p>	

	<p>коммуникационные технологии и программные средства для решения стандартных задач профессиональной деятельности на основе библиографической культуры</p>	<p>деятельности на основе библиографической культуры. Умеет: - применять приемы и методы информационной коммуникации и программные средства для решения стандартных задач профессиональной деятельности на основе библиографической культуры. Владеет: - навыками информационной коммуникации и</p> <p>и программными средствами для решения стандартных задач профессиональной деятельности на основе библиографической культуры.</p>	
<p>ПК-4.</p> <p>Способен организовывать и осуществлять деятельность, направленную на укрепление общероссийской гражданской идентичности, сохранение этнокультурного многообразия народов Российской Федерации межнационального (межэтнического) и межрелигиозного согласия, социальную и культурную адаптацию и интеграцию мигрантов.</p>	<p>ПК-4.1.</p> <p>Способен организовывать и осуществлять деятельность, направленную на укрепление общероссийской гражданской идентичности, сохранение этнокультурного многообразия народов Российской Федерации межнационального (межэтнического) и межрелигиозного согласия.</p>	<p>Знает - технику организации и осуществления деятельности, направленной на укрепление общероссийской гражданской идентичности, сохранение этнокультурного многообразия народов Российской Федерации межнационального (межэтнического) и межрелигиозного согласия. Умеет - организовывать и осуществлять деятельность, направленную на укрепление общероссийской гражданской идентичности, сохранение этнокультурного многообразия народов Российской Федерации межнационального (межэтнического) и межрелигиозного согласия. Владеет - навыками организации и осуществ-</p>	<p>Круглый стол Лекция-дискуссия Творческая работа (эссе)</p>

		ления деятельность, направленной на укрепление общероссийской гражданской идентичности, сохранение этнокультурного многообразия народов Российской Федерации межнационального (межэтнического) и межрелигиозного согласия	
	ПК-4.2. Способен организовывать и осуществлять деятельность, направленную на социальную и культурную адаптацию и интеграцию мигрантов.	Знает Технику организации и осуществления деятельности, направленной на социальную и культурную адаптацию и интеграцию мигрантов. Умеет - организовывать и осуществлять деятельность, направленную на социальную и культурную адаптацию и интеграцию мигрантов. Владеет -навыками организации и осуществления деятельности, направленной на социальную и культурную адаптацию и интеграцию мигрантов.	

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетных единиц, 72 академических часов.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы т/к успеваемости Форма промежут. аттестации(по семестрам)
			Лекции	Практ. занятия	Лаборат. занятия	Контроль самост. раб.		
№	Модуль I. Основные составляющие информационной безопасности							

1	Введение в информационную безопасность.	3	2	2		6	Устный опрос Реферат
2	Правовое обеспечение информационной безопасности.	3	2	2		6	Тестирование
3	Организационное обеспечение информационной безопасности.	3	1	1		6	Устный опрос Реферат
4	Технические средства и методы защиты информации.	3	1	1		6	
	<i>Итого по модулю 1: 36 ч.</i>		6	6		24	
Модуль II. Сетевая безопасность							
5	Настройка безопасного сетевого соединения	3	4	4		4	Коллоквиум
6	Криптографические методы защиты информации.	3	4	4		2	Реферат Устный опрос
7	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	3	1	1		2	Тестирование
8	Реализация работы инфраструктуры открытых ключей.	3	1	1		2	Реферат Диспут
9	Антивирусные средства защиты информации		2	2		2	
	<i>Итого по модулю 2: 36 ч.</i>		12	12		12	зачет
	Итого: 72 ч.		18	18		36	зачет

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Модуль I. Основные составляющие информационной безопасности

Тема 1. Введение в информационную безопасность

Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации.

Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты.

Программные и программно-аппаратные методы и средства обеспечения информационной безопасности Модели информационной безопасности.

Виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 3. Организационное обеспечение информационной безопасности

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Тема 4. Технические средства и методы защиты информации

Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Модуль II. Сетевая безопасность

Тема 5. Настройка безопасного сетевого соединения

Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS. Создание защищенного канала связи средствами виртуальной частной сети.

Тема 6. Криптографические методы защиты информации

Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA Симметричные и ассиметричные системы шифрования. Цифровые

подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы

Тема 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.

Тема 8. Реализация работы инфраструктуры открытых ключей

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Тема 9. Антивирусные средства защиты информации

Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы Изучение настроек средств антивирусной защиты информации.

4.3.2. Содержание практических занятий по дисциплине.

Модуль I. Основные составляющие информационной безопасности

Тема 1. Введение в информационную безопасность

1. Основные понятия информационной безопасности.
2. Классификация угроз.
3. Классификация средств защиты информации.
4. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
5. Модели информационной безопасности.
6. Виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности

1. Основные нормативно-правовые акты в области информационной безопасности.
2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 3. Организационное обеспечение информационной безопасности

1. Основные стандарты в области обеспечения информационной безопасности.
2. Политика безопасности.
3. Экономическая безопасность предприятия.

Тема 4. Технические средства и методы защиты информации

1. Инженерная защита объектов.

2. Защита информации от утечки по техническим каналам.

Модуль II. Сетевая безопасность

Тема 5. Настройка безопасного сетевого соединения

1. Защита информации в локальных сетях. Основы построения локальной компьютерной сети.
2. Уровни антивирусной защиты.
3. Схема сбора статистики в системе антивирусной защиты.
4. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись
5. Безопасность на сетевом уровне

Тема 6. Криптографические методы защиты информации

1. Введение в основы современных шифров с симметричным ключом.
2. Модульная арифметика. Алгебраические структуры.
3. Таблицы Вижинера.
4. Стандарты шифрования.

Тема 7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности

1. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.

Тема 8. Реализация работы инфраструктуры открытых ключей

1. Создание удостоверяющего центра
2. Генерация открытых и секретных ключей
3. Создание сертификатов открытых ключей
4. Создание электронной подписи, проверка электронной подписи.

Тема 9. Антивирусные средства защиты информации

1. Общие понятия антивирусной защиты.
2. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.
3. Основы работы антивирусных программ:

5. Образовательные технологии

- традиционные и интерактивные лекции
- традиционные семинары, семинары-конференции
- деловые и ролевые игры, разбор конкретных ситуаций
- консультации преподавателя
- самостоятельная работа студентов (подготовка рефератов, докладов)

6. Учебно-методическое обеспечение самостоятельной работы студентов

Основными видами самостоятельной работы студентов являются:

- работа с учебной и справочной литературой,
- конспектирование первоисточников,
- выполнение индивидуальных домашних заданий, задач и упражнений,
- изучение научной литературы по отдельным темам курса,
- подготовка рефератов, научных сообщений по темам,
- подготовка докладов к научным конференциям

Материалы для подготовки к самостоятельной работе студентов, представленные на сайте кафедры философии и социально-политических наук:

1. Перечень основной, словарно-справочной и дополнительной литературы имеется в учебно-методическом кабинете кафедры.
2. Первоисточники, обязательные и рекомендованные к конспектированию имеются в учебно-методическом кабинете кафедры.
3. Электронная версия методических указаний по организации самостоятельной работы имеется на кафедре философии и социально-политических наук факультета психологии и философии ДГУ.
4. Электронная библиотека учебных и контрольно-обучающих программ имеется на кафедре.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания

А) Тематика рефератов, докладов, эссе, научных сообщений

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 информации.
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 информации.
18. Программно-аппаратные средства обеспечения информационной 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

За подготовку реферата, доклада, сообщения студенту начисляются баллы в соответствии с критериями, представленными в таблице.

Критерий оценки	Содержание	Баллы
Новизна материала	<ul style="list-style-type: none"> - актуальность темы; - формулировка нового аспекта проблемы; - умение работать с научными и информационными источниками, систематизировать и структурировать материал; - наличие авторской позиции, самостоятельность оценок и суждений; - стилевое единство текста 	30
Обоснованность выбора источников	<ul style="list-style-type: none"> - анализ и оценка использованной литературы: научная литература (монографии и публикации в научных журналах) статистические данные 	20
Степень раскрытия сущности вопроса	<ul style="list-style-type: none"> - соответствие плана теме реферата - соответствие содержания теме реферата - полнота и глубина проведенного исследования - умение систематизировать и обобщать исследуемые источники, делать выводы - умение сопоставлять различные точки зрения по теме - способность давать характеристику и оценку отдельным политическим событиям и процессам 	30

Соблюдение требований к оформлению	<ul style="list-style-type: none"> - оформление ссылок на использованную литературу - оформление списка литературы - владение терминологией - соблюдение требований к оформлению реферата 	20
------------------------------------	---	----

Перевод баллов в пятибалльную шкалу оценок представлен в таблице.

Количество баллов	Оценка
90-100	Отлично
70-80	Хорошо
50-60	Удовлетворительно
0-40	Неудовлетворительно

В) вопросы и задания для текущего контроля и промежуточной аттестации.

1. Основные понятия информационной безопасности.
2. Основные составляющие. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Классификация защищаемой информации по степени важности и ценности.
5. Основные определения и критерии классификации угроз.
6. Законодательный уровень информационной безопасности.
7. Административный уровень информационной безопасности.
8. Содержание политики безопасности. Программа безопасности.
9. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
10. Управление рисками. Основные этапы управления рисками.
11. Методы и модели анализа угроз.
12. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
13. Основные программно-технические меры.
14. Архитектурная безопасность.
15. Идентификация и аутентификация, управление доступом.
16. Мониторинг и аудит.
17. Шифрование, контроль целостности.
18. Экранирование, анализ защищенности.
19. Классификация межсетевых экранов.
20. Обеспечение высокой доступности.

Критерии оценки опроса:

- оценка «отлично» (86-100 баллов) выставляется студенту, если показал знания теоретического материала и ответил на все вопросы;
- оценка «хорошо» (66-85 баллов) выставляется студенту, если показал знания теоретического материала и поверхностно ответил на некоторые вопросы;
- оценка «удовлетворительно» (51-65 баллов) выставляется студенту, если слабо показал знания теоретического материала и затруднился с ответом на дополнительные вопросы
- оценка «неудовлетворительно» (0-50 баллов) выставляется студенту, если он отказался от ответа или показал незнание теоретического материала и не ответил на вопрос

Критерии оценки зачёта

«Зачтено» выставляется студенту, если в ходе учебного процесса он выполняет следующие виды работ (и в совокупности модулей набирает средний бал равный – 51 и выше):

- конспектирует в отдельных тетрадях темы лекций, семинарских занятий, учебную литературу, ведёт словарь терминов, в том числе, конспектирует темы вынесенные на самостоятельное изучение;
- проявляет высокую активность на семинарских занятиях;
- регулярно получает 51 и более баллов на семинарах, тестировании и по докладно-реферативной работе;
- постоянно работает с вопросами для самопроверки;
- углубляет и расширяет теоретико-методологические знания;
- формирует самостоятельное мышление и т.д.

«Не зачтено» выставляется студенту, если студент пропускает занятия, небрежно ведёт или не ведёт вовсе тетради, не готовится к занятиям, не выполняет задания, или выполняет их формально, не отвечает на задаваемые вопросы.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля и промежуточного контроля.

Текущий контроль по дисциплине включает **60 баллов**:

- посещение занятий - 5 баллов
- наличие конспектов – 5 баллов
- активное участие на практических занятиях - 25 баллов
- фронтальный опрос – 10 баллов
- работа с первоисточниками, выполнение самостоятельной работы – 10 баллов
- активность на платформе MOODLE- 5 баллов

Промежуточный контроль по дисциплине включает **40 баллов**:

- коллоквиум – 20 баллов
- письменная контрольная работа или тестирование – 20 баллов

8. Учебно-методическое обеспечение дисциплины

А) Адрес сайта курса

http://dgu.ru/sveden/OOP_DGU

Б) Основная литература:

1. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с.: табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428605> – Текст : электронный.
2. Башлы, П. Н. Информационная безопасность: учебно-практическое пособие : учебное пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=90539> – ISBN 978-5-374-00301-7. – Текст: электронный.
3. Ефремов, И. В. Информационные технологии в сфере безопасности: практикум: учебное пособие / И. В. Ефремов, В. А. Солопова; Оренбургский государственный университет. – Оренбург: Оренбургский государственный университет, 2013. – 116 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=259178> – Текст: электронный.
4. Ковалев, Д. В. Информационная безопасность: учебное пособие: [16+] / Д. В. Ковалев, Е. А. Богданова; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с.: схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=493175> – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.
5. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.
6. Прохорова, О. В. Информационная безопасность и защита информации: учебник: [16+] / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.: табл., схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=438331> – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

б) дополнительная литература

1. Актуальные проблемы информационного права: практикум: учебное пособие: [16+] / сост. Л. Э. Боташева, М. С. Трофимов, О. А. Проводина, А. С. Кирпа и др. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2018. – 92 с.: ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562817> – Библиогр. в кн. – Текст: электронный.
2. Основы национальной безопасности: учебное пособие / Н. Д. Эриашвили, Е. Н. Хазов, Л. Т. Чихладзе и др.; под ред. Е. Н. Хазова, Н. Д. Эриашвили. – Москва : Юнити, 2018. – 335 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=473285>

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

Ниже приведен список адресов, ресурсы которых позволяют получить широкий доступ к электронным вариантам самых разных философских текстов:

- 1) eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – Москва, 1999 – . Режим доступа: <http://elibrary.ru/defaultx.asp>
- 2) Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.dgu.ru/>
- 3) Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: <http://elib.dgu.ru>

10. Методические указания для обучающихся по освоению дисциплины.

В ходе учебного процесса студент выполняет следующие виды работ:

- конспектирование лекций и учебной литературы;
- проработка учебного материала (по конспектам лекций учебной и научной литературе) и подготовка докладов на семинарах и практических занятиях, к участию в тематических дискуссиях и деловых играх;
- поиск и обзор научных публикаций и электронных источников информации, подготовка заключения по тематическому обзору;
- выполнение контрольных работ, творческих эссе, рефератов, др. учебных заданий,
- решение тестовых заданий;
- работа с политологическими словарями, справочниками, энциклопедиями;
- работа с вопросами для самопроверки;
- моделирование и/или анализ конкретных проблемных ситуаций ситуации;

Самостоятельная работа студентов направлена на решение следующих задач:

- углубления и расширения теоретико-методологических знаний;
- развития познавательных способностей и активности студентов, творческой инициативы, самостоятельности, ответственности, организованности;
- формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Самостоятельная работа выступает в формах анализа и обобщения студентом прочитанного на лекциях учебного материала, подготовки к семинарским занятиям, проработки вопросов и тем, представленных программой для самостоятельного изучения, подготовки докладов, устных сообщений, рефератов и др. В процессе самостоятельной работы закрепляются и совершенствуются умения и навыки студентов, полученные на лекциях и семинарских занятиях, более глубоко прорабатывается учебный материал, осмысливаются полученные на лекциях и семинарских занятиях знания. Кроме обычной самостоятельной работы, существует такая её форма как управляемая самостоятельная работа студента. Особенностью её является то, что она ведётся под контролем преподавателя.

Преподаватель определяет задания и даёт рекомендации по её выполнению, а также проверяет её результаты. Управляемая самостоятельная работа используется обычно для изучения более важных вопросов курса. В процессе проведения любой формы самостоятельной работы студент может обращаться за консультацией к преподавателю по тем или иным интересующим его или вызвавшим затруднение вопросам.

Индивидуальная работа проводится преподавателем с отдельными студентами, как правило, с целью ликвидации каких-либо пробелов в знаниях или с целью их дальнейшего углубления. В процессе индивидуальной работы развиваются умения и навыки студентов в изучении предмета, вырабатываются собственные представления по тем или иным проблемам курса.

Основная учебная литература и методические пособия имеются в читальном зале Научной библиотеки ДГУ, а также в методическом кабинете кафедры философии и социально-политических наук ДГУ. Отдельные учебные материалы также находятся на сайте кафедры (см. www.dgu.ru/). Рекомендуется также активно использовать электронные библиотеки таких учебных порталов, информационно-справочные и поисковые системы, среди которых можно назвать следующие:

- ✓ Электронно-библиотечная система IPRbooks (www.iprbookshop.ru/);
- ✓ Национальная электронная библиотека (нэб.рф)
- ✓ ЭБС Университетская библиотека ONLINE (<http://biblioclub.ru/>)

Перечень рекомендуемой литературы к учебно-методической подготовке студентов в ходе самостоятельной работы и электронные средства обучения (в частности, электронный учебник по политологии, электронный политологический словарь и др.) предоставляются студентам во время практических занятий.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Office (Access, Excel, PowerPoint, Word ит. д);
2. Дистанционное взаимодействие со студентами;
3. Образовательная платформа ДГУ MOODL;
4. Образовательный блог для изучения курса "Философии"*;
5. Полезные ссылки журналов и сайтов по философии*;
6. Программное обеспечение электронного ресурса ДГУ;
7. Статьи из журналов перечня ВАК профессорско-преподавательского состава кафедры*;
8. Электронное издание УМК*.

*Информация вывешена на сайте кафедры философии и социально-политических наук в разделах: образовательный блог, публикации, полезные ссылки.

Прямая ссылка кафедры

<http://cathedra.dgu.ru/?id=1479>

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Материально-техническое обеспечение дисциплины

- компьютерный класс факультета,
- Интернет-центр ДГУ,
- учебно-методический кабинет кафедры, оснащенный мультимедийным оборудованием.