Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность и защита персональных данных сотрудников

Направление подготовки	Управление персоналом
Код	38.03.03
Направленность (профиль)	Управление персоналом организации и государственной службы
Квалификация выпускника	бакалавр

Москва
2021

1. Перечень кодов компетенций, формируемых дисциплиной в процессе освоения образовательной программы

Группа компетенций	**Категория компетенций**	**Код**
Профессиональные		ПК-7

2. Компетенции и индикаторы их достижения

Код компетенции	**Формулировка компетенции**	**Индикаторы достижения компетенции**
ПК-7	Способен вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, составлять кадровую отчетность, обеспечить защиту персональных данных сотрудников, оптимизировать оптимизации документооборот и схемы функциональных взаимосвязей между подразделениями	ПК-7.1 ведет кадровое делопроизводство и организовывает архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами ПК-7.2 участвует в составлении кадровой отчетности, обеспечивает защиту персональных данных сотрудников, оптимизирует документооборот и схемы функциональных взаимосвязей между подразделениями

3. Описание планируемых результатов обучения по дисциплине и критериев оценки результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине.

Планируемые результаты обучения по дисциплине представлены дескрипторами (знания, умения, навыки).

Дескрипторы по дисциплине	**Знать**	**Уметь**	**Владеть**
Код компетенции	ПК-7		
	основы кадровой статистики, основы разработки и внедрения кадровой и	вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии	навыками составления кадровой отчетности, а также навыками ознакомления сотрудников

	управленческой документации; нормативно - законодательную базу и стандарты в области информационной безопасности и защиты данных сотрудников; Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	с действующими нормативно-правовыми актами, обеспечивать защиту персональных данных сотрудников; реализовывать Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	организации с кадровой документацией и действующими локальными нормативными актами; навыками оптимизации документооборота и схем функциональных взаимосвязей между подразделениями; навыками защиты персональных данных сотрудников; навыками реализации методов и средств обеспечения информационной безопасности и защиты данных сотрудников

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность и защита персональных данных сотрудников» является дисциплиной части, формируемой участниками образовательных отношений учебного плана ОПОП. Дисциплина находится в логической и содержательно-методической взаимосвязи с такими, как: «Регламентация и нормирование труда», «Информационные технологии в профессиональной деятельности», «Современные методы оценки персонала», «Управление карьерой», «Управление социальным развитием персонала».

Изучение дисциплины позволит обучающимся реализовывать профессиональные компетенции в профессиональной деятельности.

В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов: организационно-управленческий.

Профиль (направленность) программы установлен путем его ориентации на сферу профессиональной деятельности выпускников: Управление персоналом организации и государственной службы.

5. Объем дисциплины

Виды учебной работы	***Формы обучения***
	Очная
Общая трудоемкость: зачетные единицы/часы	3/108
Контактная работа:	54
Занятия лекционного типа	18
Занятия семинарского типа	36
Промежуточная аттестация: зачет	0,1
Самостоятельная работа (СРС)	53,9

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

6.1.Распределение часов по разделам/темам и видам работы

6.1.1.Очная форма обучения

№ п/п	Раздел/тема	Виды учебной работы (в часах)						
		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные занятия*	
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ	2		4				10
2.	Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников	4		8				10
3.	Угрозы информационной безопасности, их классификация и анализ.	4		6				10
4.	Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	2		6				7
5.	Информационная безопасность автоматизированных систем	2		6				7
6.	Информационная безопасность компьютеров и компьютерных	4		6				9,9

	сетей							
Итого		18		36				53,9
Промежуточная аттестация		0,1						

6.2.Программа дисциплины, структурированная по темам / разделам

6.2.1.Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	*Содержание лекционного занятия*
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ	Цели и задачи курса, общая характеристика его содержания. Основные понятия и определения. Понятие национальной и информационной безопасности РФ. Основные составляющие информационной безопасности в организации и на государственной и муниципальной службе. Национальные интересы, безопасность и основные угрозы безопасности России в информационной сфере. Государственная информационная политика. Государственная тайна. Место информационной безопасности экономических систем в национальной безопасности страны.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников	Основные нормативно-справочные документы. Законодательная база информационной безопасности и защиты данных сотрудников. Доктрина информационной безопасности РФ. Отечественные и зарубежные стандарты в области информационной безопасности. Руководящие документы Федеральной службы по техническому и экспортному контролю.
3.	Угрозы информационной безопасности, их классификация и анализ	Понятие угрозы. Виды угроз. Нарушители информационной безопасности. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз. Классификация угроз по способам их негативного воздействия и на основе методов системного анализа. Классификация атак, уровни безопасности.
4.	Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	Организационно-административные, технические, криптографические методы защиты информации. Модели каналов передачи информации. Коды, обнаруживающие и исправляющие ошибки. Защита информации в автоматизированных системах обработки данных. Аппаратная и программная реализация симметричных и асимметричных криптографических систем. Защита системы и данных в современных ОС. Механизмы информационной безопасности Идентификация и аутентификация, управление доступом.
5.	Информационная безопасность	Информационные системы и связанные с их функционированием угрозы. Причины нарушения

	автоматизированных систем	целостности информации и возможные злоумышленные действия в автоматизированных системах обработки данных. Модель нарушителя информационных систем. Модели информационной безопасности и их использование. Таксономия и анализ способов нарушения информационной безопасности. Модели оценки угроз. Модели защиты информации. Методы определения требований к защите информации. Функции и стратегии защиты информации. Архитектура систем защиты информации.
6.	Информационная безопасность компьютеров и компьютерных сетей	Цели, функции и задачи защиты информации в компьютерах и компьютерных сетях. Информационная безопасность в условиях функционирования в России глобальных сетей. Архитектура механизмов защиты информации. Разработка защищенных приложений в средах программирования. Принципы и средства защиты электронной почты. Методы защиты межсетевого обмена данными, использование межсетевых экранов. Компьютерные вирусы и их классификация. Способы заражения программ. Методы защиты. Антивирусные программы. Программно-технические средства защиты информации в компьютере.

6.2.2.Содержание практических занятий

№ п/п	**Наименование темы (раздела) дисциплины**	***Содержание практического занятия***
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ	1. Основные составляющие информационной безопасности. 2. Интересы и угрозы в области национальной безопасности. 3. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. 4. Задачи защиты информации на современном этапе 5. Основные положения государственной информационной политики.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников	1. Что такое законодательный уровень информационной безопасности? 2. В чем состоит отличительная особенность стандарта шифрования AESот DES? 3. Что собой представляет конфиденциальная информация? 4. Что собой представляет электронная подпись? 5. Какие виды требований входят в «Общие

		критерии»?
3.	Угрозы информационной безопасности, их классификация и анализ	1. Назовите наиболее выраженные угрозы информационной безопасности 2. Каков характер происхождения угроз? 3. Каковы предпосылки появления угроз? 4. Назовите известные вам подходы к классификации угроз. 5. Классификация угроз по способам их негативного воздействия.
4.	Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	1. **Что относится к основным аспектам информационной безопасности?** 2. **Что собой представляют криптографические методы и средства защиты информации?** 3. **Административный уровень информационной безопасности.** 4. **Основные классы мер процедурного уровня** 5. **Основные понятия программно-технического уровня информационной безопасности.**
5.	Информационная безопасность автоматизированных систем	**1. Что такое модель безопасности?** **2. Методы оценки уязвимости информации.** **3. Методы создания защищенных систем обработки информации.** **4. Модели политик безопасности и их сравнение.** 5. Составляющие теоретических основ методов защиты информационных
6.	Информационная безопасность компьютеров и компьютерных сетей	1. Задачи защиты информации в компьютерах и компьютерных сетях. 2. Что такое криптографические протоколы? 3. Каковы функции межсетевого экрана? 4. Программно-технические средства защиты информации в ПК 5. Классификация компьютерных вирусов.

6.2.3.Содержание самостоятельной работы

№ п/п	**Наименование темы (раздела) дисциплины**	***Содержание самостоятельной работы***
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ	Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. Цели и задачи курса, общая характеристика его содержания. Основные понятия и определения. Понятие национальной и информационной безопасности РФ. Основные составляющие информационной безопасности в организации и на

		государственной и муниципальной службе. Национальные интересы, безопасность и основные угрозы безопасности России в информационной сфере. Государственная информационная политика. Государственная тайна. Место информационной безопасности экономических систем в национальной безопасности страны.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников	Законодательный уровень информационной безопасности. Основные нормативно-справочные документы. Законодательная база информационной безопасности и защиты данных сотрудников. Доктрина информационной безопасности РФ. Отечественные и зарубежные стандарты в области информационной безопасности. Руководящие документы Федеральной службы по техническому и экспортному контролю.
3.	Угрозы информационной безопасности, их классификация и анализ	Классификация угроз. Анализ угроз информационной безопасности. Понятие угрозы. Виды угроз. Нарушители информационной безопасности. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз. Классификация угроз по способам их негативного воздействия и на основе методов системного анализа. Классификация атак, уровни безопасности.
4.	Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	Административный уровень информационной безопасности. Организационно-административные, технические, криптографические методы защиты информации. Модели каналов передачи информации. Коды, обнаруживающие и исправляющие ошибки. Защита информации в автоматизированных системах обработки данных. Аппаратная и программная реализация симметричных и асимметричных криптографических систем. Защита системы и данных в современных ОС. Механизмы информационной безопасности Идентификация и аутентификация, управление доступом.
5.	Информационная безопасность автоматизированных систем	Модели политик безопасности и их сравнение Информационные системы и связанные с их функционированием угрозы. Причины нарушения целостности информации и возможные злоумышленные действия в автоматизированных системах обработки данных. Модель нарушителя информационных систем. Модели информационной безопасности и их использование. Таксономия и анализ способов нарушения информационной безопасности. Модели оценки угроз. Модели защиты информации. Методы определения требований к защите информации. Функции и стратегии защиты информации. Архитектура систем

		защиты информации.
6.	Информационная безопасность компьютеров и компьютерных сетей	Цели, функции и задачи защиты информации в компьютерах и компьютерных сетях. Информационная безопасность в условиях функционирования в России глобальных сетей. Архитектура механизмов защиты информации. Разработка защищенных приложений в средах программирования. Принципы и средства защиты электронной почты. Методы защиты межсетевого обмена данными, использование межсетевых экранов. Компьютерные вирусы и их классификация. Способы заражения программ. Методы защиты. Антивирусные программы. Программно-технические средства защиты информации в компьютере. Компьютерные вирусы и их классификация. Способы заражения программ. Методы защиты. Антивирусные программы. Программно-технические средства защиты информации в ПК

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Предусмотрены следующие виды контроля качества освоения конкретной дисциплины:
- текущий контроль успеваемости
- промежуточная аттестация обучающихся по дисциплине

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен в **ПРИЛОЖЕНИИ** к РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины в процессе обучения.

7.1 Паспорт фонда оценочных средств для проведения текущей аттестации по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ	Опрос, проблемно-аналитические задания
2.	Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников	Опрос, проблемно-аналитические задания, информационный проект, тест

3.	Угрозы информационной безопасности, их классификация и анализ	Опрос, проблемно-аналитические задания, информационный проект
4.	Методы и средства обеспечения информационной безопасности и защиты данных сотрудников	Опрос, проблемно-аналитические задания, тест
5.	Информационная безопасность автоматизированных систем	Опрос, проблемно-аналитические задания, информационный проект
6.	Информационная безопасность компьютеров и компьютерных сетей	Опрос, проблемно-аналитические задания, тест

*7.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе текущего к**о**нтроля*

Типовые вопросы

1. Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.
2. Основные составляющие информационной безопасности.
3. Интересы и угрозы в области национальной безопасности.
4. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
5. Задачи защиты информации на современном этапе
6. Основные положения государственной информационной политики. Нормативно - законодательная база и стандарты в области информационной безопасности и защиты данных сотрудников
7. Что такое законодательный уровень информационной безопасности?
8. В чем состоит отличительная особенность стандарта шифрования AESот DES?
9. Что собой представляет конфиденциальная информация?
10. Что собой представляет электронная подпись?
11. Какие виды требований входят в «Общие критерии»?
12. Что относится к персональным данным сотрудников.
13. Угрозы информационной безопасности, их классификация и анализ
14. Назовите наиболее выраженные угрозы информационной безопасности
15. Каков характер происхождения угроз?
16. Каковы предпосылки появления угроз?
17. Назовите известные вам подходы к классификации угроз.
18. Классификация угроз по способам их негативного воздействия.
19. Методы и средства обеспечения информационной безопасности и защиты данных сотрудников
20. Что относится к основным аспектам информационной безопасности?
21. Что собой представляют криптографические методы и средства защиты информации?
22. Административный уровень информационной безопасности.
23. Основные классы мер процедурного уровня
24. Основные понятия программно-технического уровня информационной безопасности.
25. Информационная безопасность компьютеров и компьютерных сетей
26. Задачи защиты информации в компьютерах и компьютерных сетях.
27. Что такое криптографические протоколы?

28. Каковы функции межсетевого экрана?
29. Программно-технические средства защиты информации в ПК
30. Классификация компьютерных вирусов.

Проблемно-аналитические задания:

Задание №1

Исходя из анализа описания, программной и технической архитектуры предприятия определить комплекс средств инженерно-технической защиты информации необходимый для существенного повышения уровня ее защиты.

Задание №2:

1. Проанализируйте нормативно-правовую базу, регулирующую защиту персональных данных сотрудников организации. Сформируйте соответствующий перечень документов.

2. Опишите процедуру оформления электронной подписи для физических и юридических лиц.

Задание №3

Исходя из анализа описания предприятия определить и ранжировать его основные активы. Результаты представить в виде таблиц.

Задание №4

Исходя из анализа предложенной политики информационной безопасности, определить ее упущения и слабые места.

Задание №5

Исходя из анализа описания предприятия определить перечень информационных активов, обязательное ограничение доступа к которым регламентируется действующим законодательством РФ, а также отнесенных к коммерческой тайне.

Задание №6

Исходя из анализа описания предприятия и его основных активов определить соответствующие уязвимости. Результаты представить в виде таблицы.

Задание №7

Исходя из анализа описания, программной и технической архитектуры предприятия определить возможные каналы утечки информации, являющейся коммерческой тайной.

Задание №8

Исходя из анализа описания предприятия и его основных активов, определить соответствующие угрозы. Результаты представить в виде таблицы.

Задание №9

Исходя из анализа описания предприятия и его основных активов, уязвимостей и угроз определить и ранжировать соответствующие риски. Результаты представить в виде таблицы.

Задание №10

На примере одной из организаций подготовить информационный проект на тему «Защита данных сотрудников организации»

Задание №11

Просчитайте примерную стоимость минимального набора программного обеспечения для обеспечения информационной безопасности и защиты данных персонала организации из 20 сотрудников. Результат представьте в виде таблицы.

Задание №12

Исходя из анализа потенциальных каналов утечки информации, являющейся конфиденциальной, а также представляющей коммерческую либо государственную тайну определить перечень мер по предотвращению возможной утечки (включая установку аппаратных и программных средств).

Задание №13

По представленным данным о затратах на систему обеспечения информационной безопасности провести расчет показателей ее экономической эффективности.

Темы информационных проектов

Подготовка и защита информационного проекта:

1. Нормативно - законодательная база и стандарты в области информационной безопасности
2. Угрозы информационной безопасности, их классификация и анализ.
3. Методы и средства обеспечения информационной безопасности.
4. Информационная безопасность компьютеров и компьютерных сетей
5. Основные задачи и проблемы информационной безопасности
6. Киберпреступность
7. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.
8. Угрозы информационной безопасности и управление рисками.
9. Причины, виды, каналы утечки и искажения информации.
10. Технические каналы утечки информации.

Подготовка и защита исследовательского проекта:

1. Технические средства обеспечения безопасности объекта.
2. Программно-аппаратные средства обеспечения информационной безопасности.
3. Методы контроля доступа к информации.
4. Вредоносные программы.
5. Основы криптографической защиты информации.
6. Обеспечение информационной безопасности операционных систем
7. Основы безопасности сетевых технологий.
8. Организационно-правовое обеспечение защиты информации.
9. Стандарты информационной безопасности
10. Информация как наиболее ценный ресурс современного общества.
11. Актуальность и значимость информационной безопасности.
12. Государственная информационная политика РФ.

Типовые тесты

1. Какие существуют основные уровни обеспечения защиты информации?

1) законодательный
2) административный
3) программно-технический
4) вероятностный
5) процедурный

2. С чем связана основная причина потерь информации в компьютерных сетях?
1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности
4) с плохими законами

3. К аспектам ИБ относятся:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

4. Что такое несанкционированный доступ?
1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2) Создание резервных копий в организации
3) Правила для обхода парольной защиты
4) Вход в систему без согласования с руководителем организации
5) Удаление не нужной информации

5. Что такое целостность информации?
1) возможность ее изменения любым субъектом
2) возможность изменения только единственным пользователем
3) существование в виде единого набора файлов
4) существование в неискаженном виде

6. Что такое аутентификация?
1) Проверка количества переданной и принятой информации
2) Проверка подлинности идентификации
3) Проверка подлинности информации
4) Определение файлов, из которых удалена служебная информация

7. Утечка информации
1) несанкционированное изменение информации
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря данных
4) уменьшение объема информации

8. Основные программы для защиты от компьютерных вирусов
1) Программы-сканеры
2) Программы-мониторы
3) Программы-детекторы
4) Программы-фильтры
5) Программы-ректоры

9. Отметьте функции, которые должны осуществлять средства защиты:
1) Разграничение доступа к вычислительным ресурсам и информации
2) Несанкционированный доступ к системе
3) Идентификация субъектов и объектов
4) Разграничение вычислительных ресурсов и информации
5) Регистрация действий в системе

10. Сервисы безопасности:
1) идентификация и аутентификация
2) шифрование
3) инверсия паролей
4) контроль целостности
5) регулирование конфликтов

7.3.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Все задания, используемые для текущего контроля формирования компетенций условно можно разделить на две группы:

1. задания, которые в силу своих особенностей могут быть реализованы только в процессе обучения на занятиях (например, дискуссия, круглый стол, диспут, мини-конференция);
2. задания, которые дополняют теоретические вопросы (практические задания, проблемно-аналитические задания, тест).

Выполнение всех заданий является необходимым для формирования и контроля знаний, умений и навыком. Поэтому, в случае невыполнения заданий в процессе обучения, их необходимо «отработать» до зачета (экзамена). Вид заданий, которые необходимо выполнить для ликвидации «задолженности» определяется в индивидуальном порядке, с учетом причин невыполнения.

1)Требование к теоретическому устному ответу

Оценка знаний предполагает дифференцированный подход к студенту, учет его индивидуальных способностей, степень усвоения и систематизации основных понятий и категорий по дисциплине. Кроме того, оценивается не только глубина знаний поставленных вопросов, но и умение использовать в ответе практический материал. Оценивается культура речи, владение навыками ораторского искусства.

Критерии оценивания: последовательность, полнота, логичность изложения, анализ различных точек зрения, самостоятельное обобщение материала, использование профессиональных терминов, культура речи, навыки ораторского искусства. Изложение материала без фактических ошибок.

Оценка *«отлично»* ставится в случае, когда материал излагается исчерпывающе, последовательно, грамотно и логически стройно, при этом раскрываются не только основные понятия, но и анализируются точки зрения различных авторов. Обучающийся не затрудняется с ответом, соблюдает культуру речи.

Оценка *«хорошо»* ставится, если обучающийся твердо знает материал, грамотно и по существу излагает его, знает практическую базу, но при ответе на вопрос допускает несущественные погрешности.

Оценка *«удовлетворительно»* ставится, если обучающийся освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении материала, затрудняется с ответами, показывает отсутствие должной связи между анализом, аргументацией и выводами.

Оценка *«неудовлетворительно»* ставится, если обучающийся не отвечает на поставленные вопросы.

2) Творческие задания

Эссе – это небольшая по объему письменная работа, сочетающая свободные,

субъективные рассуждения по определенной теме с элементами научного анализа. Текст должен быть легко читаем, но необходимо избегать нарочито разговорного стиля, сленга, шаблонных фраз. Объем эссе составляет примерно 2 – 2,5 стр. 12 шрифтом с одинарным интервалом (без учета титульного листа).

Критерии оценивания - оценка учитывает соблюдение жанровой специфики эссе, наличие логической структуры построения текста, наличие авторской позиции, ее научность и связь с современным пониманием вопроса, адекватность аргументов, стиль изложения, оформление работы. Следует помнить, что прямое заимствование (без оформления цитат) текста из Интернета или электронной библиотеки недопустимо.

Оценка *«отлично»* ставится в случае, когда определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения); наличие четко определенной личной позиции по теме эссе; адекватность аргументов при обосновании личной позиции, стиль изложения.

Оценка *«хорошо»* ставится, когда в целом определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения); но не прослеживается наличие четко определенной личной позиции по теме эссе; не достаточно аргументов при обосновании личной позиции

Оценка *«удовлетворительно»* ставится, когда в целом определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение). Но не прослеживаются четкие выводы, нарушается стиль изложения

Оценка *«неудовлетворительно»* ставится, если не выполнены никакие требования

3) Требование к решению ситуационной, проблемной задачи (кейс-измерители)

Студент должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи должны решаться студентами письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка *«отлично»* ставится в случае, когда обучающийся выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка *«хорошо»* ставится, если обучающийся в целом выполнил все требования, но не совсем четко определяется опора на теоретические положения, изложенные в научной литературе по данному вопросу.

Оценка *«удовлетворительно»* ставится, если обучающийся показал положительные результаты в процессе решения задачи.

Оценка *«неудовлетворительно»* ставится, если обучающийся не выполнил все требования.

4) Интерактивные задания

Механизм проведения диспут-игры (ролевой (деловой) игры).

Необходимо разбиться на несколько команд, которые должны поочередно высказать свое мнение по каждому из заданных вопросов. Мнение высказывающейся команды засчитывается, если противоположная команда не опровергнет его контраргументами. Команда, чье мнение засчитано как верное (не получило убедительных контраргументов от противоположных команд), получает один балл. Команда, опровергнувшая мнение противоположной команды своими контраргументами, также получает один балл.

Побеждает команда, получившая максимальное количество баллов.

Ролевая игра, как правило, имеет фабулу (ситуацию, казус), распределяются роли, подготовка осуществляется за 2-3 недели до проведения игры.

Критерии оценивания – оцениваются действия всех участников группы. Понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Соответствие реальной действительности решений, выработанных в ходе игры. Владение терминологией, демонстрация владения учебным материалом по теме игры, владение методами аргументации, умение работать в группе (умение слушать, конструктивно вести беседу, убеждать, управлять временем, бесконфликтно общаться), достижение игровых целей, (соответствие роли – при ролевой игре). Ясность и стиль изложения.

Оценка *«отлично»* ставится в случае, выполнения всех критериев.

Оценка *«хорошо»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Решения, выработанные в ходе игры, полностью соответствуют реальной действительности. Но некоторые объяснения не совсем аргументированы, нарушены нормы общения, нарушены временные рамки, нарушен стиль изложения.

Оценка *«удовлетворительно»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия в целом соответствуют заданным целям. Однако, решения, выработанные в ходе игры, не совсем соответствуют реальной действительности. Некоторые объяснения не совсем аргументированы, нарушены временные рамки, нарушен стиль изложения.

Оценка *«неудовлетворительно»* ставится, если обучающиеся не понимают проблему, их высказывания не соответствуют заданным целям.

5) Комплексное проблемно-аналитическое задание

Задание носит проблемно-аналитический характер и выполняется в три этапа. На первом из них необходимо ознакомиться со специальной литературой.

Целесообразно также повторить учебные материалы лекций и семинарских занятий по темам, в рамках которых предлагается выполнение данного задания.

На втором этапе выполнения работы необходимо сформулировать проблему и изложить авторскую версию ее решения, на основе полученной на первом этапе информации.

Третий этап работы заключается в формулировке собственной точки зрения по проблеме. Результат третьего этапа оформляется в виде аналитической записки (объем: 2-2,5 стр.; 14 шрифт, 1,5 интервал).

Критерий оценивания - оценка учитывает: понимание проблемы, уровень раскрытия поставленной проблемы в плоскости теории изучаемой дисциплины, умение формулировать и аргументировано представлять собственную точку зрения, выполнение всех этапов работы.

Оценка *«отлично»* ставится в случае, когда обучающийся демонстрирует полное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«хорошо»* ставится, если обучающийся демонстрирует значительное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«удовлетворительно»* ставится, если обучающийся, демонстрирует частичное понимание проблемы, большинство требований, предъявляемых к заданию, выполнены

Оценка *«неудовлетворительно»* ставится, если обучающийся демонстрирует непонимание проблемы, многие требования, предъявляемые к заданию, не выполнены.

6) Исследовательский проект

Исследовательский проект **–** проект, структура которого приближена к формату научного исследования и содержит доказательство актуальности избранной темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, историографии, обобщение результатов, выводы.

Результаты выполнения исследовательского проекта оформляется в виде реферата (объем: 12-15 страниц.; 14 шрифт, 1,5 интервал).

Критерии оценивания - поскольку структура исследовательского проекта максимально приближена к формату научного исследования, то при выставлении учитывается доказательство актуальности темы исследования, определение научной проблемы, объекта и предмета исследования, целей и задач, источников, методов исследования, выдвижение гипотезы, обобщение результатов и формулирование выводов, обозначение перспектив дальнейшего исследования.

Оценка *«отлично»* ставится в случае, когда обучающийся демонстрирует полное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«хорошо»* ставится, если обучающийся демонстрирует значительное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«удовлетворительно»* ставится, если обучающийся, демонстрирует частичное понимание проблемы, большинство требований, предъявляемых к заданию, выполнены

Оценка *«неудовлетворительно»* ставится, если обучающийся демонстрирует непонимание проблемы, многие требования, предъявляемые к заданию, не выполнены.

7) Информационный проект (презентация)

Информационный проект **–** проект, направленный на стимулирование учебно-познавательной деятельности студента с выраженной эвристической направленностью (поиск, отбор и систематизация информации об объекте, оформление ее для презентации). Итоговым продуктом проекта может быть письменный реферат, электронный реферат с иллюстрациями, слайд-шоу, мини-фильм, презентация и т.д.

Информационный проект отличается от исследовательского проекта, поскольку представляет собой такую форму учебно-познавательной деятельности, которая отличается ярко выраженной эвристической направленностью.

Критерии оценивания - при выставлении оценки учитывается самостоятельный поиск, отбор и систематизация информации, раскрытие вопроса (проблемы), ознакомление студенческой аудитории с этой информацией (представление информации), ее анализ и обобщение, оформление, полные ответы на вопросы аудитории с примерами.

Оценка *«отлично»* ставится в случае, когда обучающийся полностью раскрывает вопрос (проблему), представляет информацию систематизировано, последовательно, логично, взаимосвязано, использует более 5 профессиональных терминов, широко использует информационные технологии, ошибки в информации отсутствуют, дает полные ответы на вопросы аудитории с примерами.

Оценка *«хорошо»* ставится, если обучающийся раскрывает вопрос (проблему), представляет информацию систематизировано, последовательно, логично, взаимосвязано, использует более 2 профессиональных терминов, достаточно использует информационные технологии, допускает не более 2 ошибок в изложении материала, дает полные или частично полные ответы на вопросы аудитории.

Оценка *«удовлетворительно»* ставится, если обучающийся, раскрывает вопрос (проблему) не полностью, представляет информацию не систематизировано и не совсем последовательно, использует 1-2 профессиональных термина, использует информационные технологии, допускает 3-4 ошибки в изложении материала, отвечает только на элементарные вопросы аудитории без пояснений.

Оценка *«неудовлетворительно»* ставится, если вопрос не раскрыт, представленная информация логически не связана, не используются профессиональные термины, допускает более 4 ошибок в изложении материала, не отвечает на вопросы аудитории.

8) Дискуссионные процедуры

Круглый стол, дискуссия, полемика, диспут, дебаты, мини-конференции являются средствами, позволяющими включить обучающихся в процесс обсуждения спорного

вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Задание дается заранее, определяется круг вопросов для обсуждения, группы участников этого обсуждения.

Дискуссионные процедуры могут быть использованы для того, чтобы студенты:

–лучше поняли усвояемый материал на фоне разнообразных позиций и мнений, не обязательно достигая общего мнения;

– смогли постичь смысл изучаемого материала, который иногда чувствуют интуитивно, но не могут высказать вербально, четко и ясно, или конструировать новый смысл, новую позицию;

– смогли согласовать свою позицию или действия относительно обсуждаемой проблемы.

Критерии оценивания – оцениваются действия всех участников группы. Понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Соответствие реальной действительности решений, выработанных в ходе игры. Владение терминологией, демонстрация владения учебным материалом по теме игры, владение методами аргументации, умение работать в группе (умение слушать, конструктивно вести беседу, убеждать, управлять временем, бесконфликтно общаться), достижение игровых целей, (соответствие роли – при ролевой игре). Ясность и стиль изложения.

Оценка *«отлично»* ставится в случае, когда все требования выполнены в полном объеме.

Оценка *«хорошо»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Решения, выработанные в ходе игры, полностью соответствуют реальной действительности. Но некоторые объяснения не совсем аргументированы, нарушены нормы общения, нарушены временные рамки, нарушен стиль изложения.

Оценка *«удовлетворительно»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия в целом соответствуют заданным целям. Однако, решения, выработанные в ходе игры, не совсем соответствуют реальной действительности. Некоторые объяснения не совсем аргументированы, нарушены временные рамки, нарушен стиль изложения.

Оценка *«неудовлетворительно»* ставится, если обучающиеся не понимают проблему, их высказывания не соответствуют заданным целям.

9) Тестирование

Является одним из средств контроля знаний обучающихся по дисциплине.

Критерии оценивания – правильный ответ на вопрос

Оценка *«отлично»* ставится в случае, если правильно выполнено 90-100% заданий

Оценка *«хорошо»* ставится, если правильно выполнено 70-89% заданий

Оценка *«удовлетворительно»* ставится в случае, если правильно выполнено 50-69% заданий

Оценка *«неудовлетворительно»* ставится, если правильно выполнено менее 50% заданий

10) Требование к письменному опросу (контрольной работе)

Оценивается не только глубина знаний поставленных вопросов, но и умение изложить письменно.

Критерии оценивания: последовательность, полнота, логичность изложения, анализ различных точек зрения, самостоятельное обобщение материала. Изложение материала без фактических ошибок.

Оценка *«отлично»* ставится в случае, когда соблюдены все критерии.

Оценка *«хорошо»* ставится, если обучающийся твердо знает материал, грамотно и по существу излагает его, знает практическую базу, но допускает несущественные

погрешности.

Оценка *«удовлетворительно»* ставится, если обучающийся освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении материала, затрудняется с ответами, показывает отсутствие должной связи между анализом, аргументацией и выводами.

Оценка *«неудовлетворительно»* ставится, если обучающийся не отвечает на поставленные вопросы.

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

8.1 Основная литература:

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89443.html
2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97562.html
3. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77320.html
4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

8.2. Дополнительная литература:

1. Алешин А.П. Техническое обеспечение безопасности бизнеса (2-е издание) [Электронный ресурс]/ Алешин А.П.— Электрон. текстовые данные.— М.: Дашков и К, Ай Пи Эр Медиа, 2017. — 160 с.— Режим доступа: http://www.iprbookshop.ru/57143 .— ЭБС «IPRbooks»
2. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/86357.html
3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере : учебное пособие / Фаронов А.Е.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89453.html

8.3. Периодические издания:

1. Журнал «Компьютерра» http://www.computerra.ru

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модуля)

1. www.iprbookshop.ru – электронно-библиотечная система
2. www.elibraru.ru -– бесплатная электронная Интернет библиотека.
3. www.Wikipedia.org – свободная энциклопедия

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекций, практических занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев полноценного высшего образования, на которую отводится значительная часть учебного времени.

Самостоятельная работа студентов складывается из следующих составляющих:

1. работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
2. внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
3. выполнение самостоятельных практических работ;
4. подготовка к экзаменам (зачетам) непосредственно перед ними.

Для правильной организации работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Задания, проблемные вопросы, предложенные для изучения дисциплины, в том числе и для самостоятельного выполнения, носят междисциплинарный характер и базируются, прежде всего, на причинно-следственных связях между компонентами окружающего нас мира. В течение семестра, необходимо подготовить рефераты (проекты) с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию также способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

При выполнении докладов, творческих, информационных, исследовательских проектов особое внимание следует обращать на подбор источников информации и методику работы с ними.

Для успешной сдачи экзамена (зачета) рекомендуется соблюдать следующие правила:

- Подготовка к экзамену (зачету) должна проводиться систематически, в течение всего семестра.
- Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.
- Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

На экзамене (зачете) высокую оценку получают студенты, использующие данные, полученные в процессе выполнения самостоятельных работ, а также использующие собственные выводы на основе изученного материала.

Учитывая значительный объем теоретического материала, студентам рекомендуется регулярное посещение и подробное конспектирование лекций.

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

1. Терминальный сервер, предоставляющий к нему доступ клиентам на базе Windows Server 2016
2. Семейство ОС Microsoft Windows
3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом
4. Информационно-справочная система: Система КонсультантПлюс (Информационный комплекс)
5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (ЭПС «Система ГАРАНТ»)
6. Антивирусная система NOD 32
7. Adobe Reader. Лицензия проприетарная свободно-распространяемая.

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

12.1 Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения.

Специализированная мебель:
Комплект учебной мебели на 30 посадочных мест; доска (маркерная) - 1шт..

Технические средства обучения:
Компьютеры в сборе - 30 шт.; компьютер в сборе для преподавателя - 1 шт., проектор, колонки, экран.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:
Windows 10, Microsoft Office 2016, Zoom, КонсультантПлюс, Система ГАРАНТ, Антивирус NOD32, 1С:Предприятие 8 (Зарплата и управление персоналом; Зарплата и кадры государственного учреждения).

Перечень свободно распространяемого программного обеспечения:
Adobe Acrobat Reader DC; Google Chrome; LibreOffice, Skype, Gimp, Paint.net, AnyLogic, Inkscape.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду ММУ.

12.2 Помещение для самостоятельной работы обучающихся.

Специализированная мебель:
Комплект учебной мебели на 5 посадочных мест, в том числе для лиц с ограниченными возможностями здоровья 2 посадочных места.

Технические средства обучения:
Компьютеры в сборе - 5 шт.; телевизор Sharp; беспроводная клавиатура Clevy с большими ярко окрашенными кнопками и разделителем для лиц с нарушениями опорно-двигательного аппарата; роллер, заменяющий компьютерную мышь, для лиц с нарушениями опорно-двигательного аппарата; видеоувеличитель электронный ручной, позволяющий читать слабовидящим людям плоскопечатный текст на мониторе (экране) с возможностью увеличения текста; портативный дисплей Брайля Focus 14 Blue, включающий точечную клавиатуру, возможность подключения по Bluetooth и USB, возможность подключения к ПК и к смартфону, руководство пользователя шрифтом Брайля; клавиатура со шрифтом Брайля;

наушники; колонки.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:
Windows 10, Zoom, КонсультантПлюс, Система ГАРАНТ, Антивирус NOD32.

Перечень свободно распространяемого программного обеспечения:
Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype.
Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ММУ.

13. Образовательные технологии, используемые при освоении дисциплины

Для освоения дисциплины используются как традиционные формы занятий – лекции (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация); и семинарские (практические) занятия, так и активные и интерактивные формы занятий - деловые и ролевые игры, решение ситуационных задач и разбор конкретных ситуаций.

На учебных занятиях используются технические средства обучения мультимедийной аудитории: компьютер, монитор, колонки, настенный экран, проектор, микрофон, пакет программ Microsoft Office для демонстрации презентаций и медиафайлов, видеопроектор для демонстрации слайдов, видеосюжетов и др. Тестирование обучаемых может осуществляться с использованием компьютерного оборудования университета.

13.1. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:
- чтение проблемно-информационных лекций с использованием доски и видеоматериалов;
- практические занятия для обсуждения, дискуссий и обмена мнениями;
- контрольные опросы;
- консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками;
- подготовка и обсуждение рефератов (проектов), презентаций (научно-исследовательская работа);
- тестирование по основным темам дисциплины.

13.2. Активные и интерактивные методы и формы обучения
Из перечня видов: («*мозговой штурм», анализ НПА, анализ проблемных ситуаций, анализ конкретных ситуаций, инциденты, имитация коллективной профессиональной деятельности, разыгрывание ролей, творческая работа, связанная с освоением дисциплины, ролевая игра, круглый стол, диспут, беседа, дискуссия, мини-конференция и др.*) используются следующие:
- *диспут*
- *анализ проблемных, творческих заданий, ситуационных задач*
- *ролевая игра;*
- *круглый стол;*
- *мини-конференция*
-*дискуссия*
- *беседа.*

13.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее –

инвалиды и лица с ОВЗ) с целью обеспечения их прав. При обучении учитываются особенности их психофизического развития, индивидуальные возможности и при необходимости обеспечивается коррекция нарушений развития и социальная адаптация указанных лиц.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально-технического обеспечения, особенностями восприятия учебной информации студентов-инвалидов и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.