Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность и защита данных

Направление подготовки	Информационные системы и технологии
Код	09.03.02
Направленность (профиль)	Информационные системы и технологии в экономике и управлении
Квалификация выпускника	бакалавр

Москва
2023

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

Группа компетенций	Категория компетенций	Код
Профессиональные		ПК-6

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-6	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения.	**ПК-6.1.** Определяет параметры безопасности и защиты программного обеспечения сетевых устройств **ПК-6.2.** Понимает принципы обеспечения безопасности и защиты программного обеспечения сетевых устройств. **ПК-6.3.** Выполняет установку и настройку специализированных программных средств обеспечения безопасности, настройку параметров безопасности операционных систем сетевых устройств. **ПК-6.4.** Понимает принципы обеспечения безопасности и защиты программного обеспечения сетевых устройств. **ПК-6.5.** Оценивает производительность сетевой инфраструктуры инфокоммуникационной системы, использует инструменты диагностики отказов и ошибок сетевых устройств.

3. Описание планируемых 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-6**		

	- виды угроз информационных систем и методы обеспечения информационной безопасности; - основы информационной безопасности организации; - параметры безопасности и защиты программного обеспечения сетевых устройств, средства управления и обеспечения безопасности администрируемой сети.	- организовать комплексную защиту информационных систем; - определять параметры безопасности и защиты программного обеспечения сетевых устройств, устанавливать и администрировать средства управления и обеспечения безопасности администрируемой сети; - выполнять контроль использования ресурсов сетевых устройств и программного обеспечения; - оценивать производительность сетевой инфраструктуры инфокоммуникационной системы и использовать инструменты диагностики отказов и ошибок сетевых устройств.	- навыками выполнения регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы, восстановления параметров программного обеспечения сетевых устройств; - средствами контроля использование ресурсов сетевых устройств и программного обеспечения; - методами настройки сетевых элементов инфокоммуникационной системы; - правовыми, административными, программно-аппаратными средствами информационной защиты, навыками работы с инструментальными средствами защиты информации.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений учебного плана ОПОП.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как «Проектирование информационных систем», «Офисные технологии», «Информационные системы и базы данных».

В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов: научно-исследовательский, производственно-технологический, организационно-управленческий, проектный.

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: информационные системы и технологии в экономике и управлении.

5. Объем дисциплины

Виды учебной работы	*Формы обучения*
	Очная
Общая трудоемкость: зачетные единицы/часы	2/72
Контактная работа:	
Занятия лекционного типа	18
Занятия семинарского типа	36
Промежуточная аттестация: **зачет**	0,1
Самостоятельная работа (СРС)	17,9

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*	
1.	Основные понятия и определения информационной безопасности.	2		4				2
2.	Понятие угрозы. Виды угроз информационной безопасности	2		4				2
3.	Понятия утечки информации.	2		4				2
4.	Криптографические методы защиты.	2		4				2
5.	Технологии аутентификации.	2		4				2
6.	Атаки на сервера и рабочие станции.	2		4				2
7.	Технологии межсетевых экранов.	2		4				1
8.	Антивирусная защита.	2		4				1
9.	Технологии построения защищенных информационных систем.	2		4				3,9

	Промежуточная аттестация	0,1						
	Итого	18		36				17,9

6.1 Программа дисциплины, структурированная по темам / разделам

6.2.1 Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1.	Основные понятия и определения информационной безопасности.	Проблема информационной безопасности. Виды защищаемой информации.
2.	Понятие угрозы. Виды угроз информационной безопасности	Характеристики информационных атак. Информационная безопасность в условиях функционирования в России глобальных сетей.
3.	Понятия утечки информации.	Основные нарушения. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.
4.	Криптографические методы защиты.	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования. Алгоритмы шифрования. Электронная цифровая подпись.
5.	Технологии аутентификации.	Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли.
6.	Атаки на сервера и рабочие станции.	Атака типа «отказ в обслуживании». Протоколирование. Настройка и использование файрволов.
7.	Технологии межсетевых экранов.	Функции межсетевых экранов и особенности их функционирования. Схемы сетевой защиты на базе межсетевых экранов.
8.	Антивирусная защита.	Объекты внедрения, режимы функционирования и специальные функции вирусов. Основные принципы использования антивирусного программного обеспечения.
9.	Технологии построения защищенных информационных систем.	Средства операционной системы. Средства резервирования данных. Проверка целостности.

6.2.2 Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основные понятия и определения информационной безопасности.	Проблема информационной безопасности. Виды защищаемой информации.
2.	Понятие угрозы. Виды угроз информационной безопасности	Характеристики информационных атак. Информационная безопасность в условиях функционирования в России глобальных сетей.

3.	Понятия утечки информации.	Основные нарушения. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.
4.	Криптографические методы защиты.	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования. Алгоритмы шифрования. Электронная цифровая подпись.
5.	Технологии аутентификации.	Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли.
6.	Атаки на сервера и рабочие станции.	Атака типа «отказ в обслуживании». Протоколирование. Настройка и использование файрволов.
7.	Технологии межсетевых экранов.	Функции межсетевых экранов и особенности их функционирования. Схемы сетевой защиты на базе межсетевых экранов.
8.	Антивирусная защита.	Объекты внедрения, режимы функционирования и специальные функции вирусов. Основные принципы использования антивирусного программного обеспечения.
9.	Технологии построения защищенных информационных систем.	Средства операционной системы. Средства резервирования данных. Проверка целостности.

6.2.3 Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основные понятия и определения информационной безопасности.	Модели информационной безопасности. Выбор средств защиты системы информационной безопасности
2.	Понятие угрозы. Виды угроз информационной безопасности	Инструменты информационных атак. Средства предупреждения атак.
3.	Понятия утечки информации.	Электромагнитные, электрические и параметрические каналы утечки информации
4.	Криптографические методы защиты.	Алгоритмы электронно-цифровой подписи. Особенности использования
5.	Технологии аутентификации.	Настройка политик, отвечающих за информационную безопасность
6.	Атаки на сервера и рабочие станции.	Сетевые защищенные протоколы. Защита от удаленных атак через сеть Internet.
7.	Технологии межсетевых экранов.	Особенности использования межсетевых экранов для обеспечения информационной безопасности
8.	Антивирусная защита.	Вопросы обновления антивирусных баз данных.
9.	Технологии построения защищенных информационных систем.	Способы и средства восстановления работоспособности.

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 и определения информационной безопасности.	Опрос, тестирование.
2.	Понятие угрозы. Виды угроз информационной безопасности	Опрос, творческий проект, тестирование.
3.	Понятия утечки информации.	Опрос, информационный проект, тестирование.
4.	Криптографические методы защиты.	Опрос, творческий проект.
5.	Технологии аутентификации.	Опрос, тестирование.
6.	Атаки на сервера и рабочие станции.	Опрос, творческий проект, тестирование.
7.	Технологии межсетевых экранов.	Опрос, тестирование.
8.	Антивирусная защита.	Опрос, информационный проект, тестирование.
9.	Технологии построения защищенных информационных систем.	Опрос, тестирование.

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

Типовые вопросы

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?

8. Что такое криптографические методы защиты информации?
9. Перечислите виды защищаемой информации.
10. Какие основные законы в области защиты информации в РФ?
11. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
12. Что такое профессиональная тайна?
13. Что такое коммерческая тайна?
14. Что такое государственная тайна?
15. Опишите правовой режим государственной тайны.
16. Как связаны международные стандарты и стандарты РФ?
17. Что такое политика безопасности?
18. Что такое инженерная защита объектов?
19. Что такое технические каналы утечки информации?
20. Перечислите основные виды технических каналов утечки информации?
21. Перечислите методы защиты информации от утечки по визуальному каналу.
22. Перечислите методы защиты информации от утечки по воздушному каналу.
23. Перечислите методы защиты информации от утечки по вибрационному каналу.
24. Перечислите методы защиты информации от утечки по индукционному каналу.
25. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
26. Что такое брандмауэр?
27. Что такое антивирусная программа?
28. Что такое эвристический алгоритм поиска вирусов?
29. Что такое сигнатурный поиск вирусов?
30. Что такое механизм контроля и разграничения доступа?
31. Что такое криптография?
32. Какие используются симметричные алгоритмы шифрования?
33. Какие используются ассиметричные алгоритмы шифрования?
34. Что такое цифровая подпись?
35. Что такое инфраструктура открытых ключей?

Темы исследовательских, творческих проектов

Подготовка исследовательских проектов по темам:

1. Методы противодействия сниффингу.
2. Средства и методы защиты информации от утечки в телефонных линиях.
3. Виды сигнализаций устанавливаются для обеспечения инженерной защиты.
4. Основные стандарты РФ в области информационной безопасности.
5. Российские и международные стандарты на формирование цифровой подписи.

Информационный проект

Подготовьте информационный проект (презентацию) по теме:

1. Инфраструктура открытых ключей.
2. Модели безопасности.
3. Виды защищаемой информации.
4. Организационное обеспечение информационной безопасности.
5. Инженерная защита и охрана объектов.

Творческое задание (с элементами эссе)

Напишите эссе по теме:

1. Основные криптографические протоколы, используемые в сетях.

2. Средства стеганографической защиты информации.
3. Программно-аппаратных средства защиты информации.
4. Основные международные стандарты в области информационной безопасности.
5. Криптографические методы защиты информации.

Типовые тесты

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
a) Разработка аппаратных средств обеспечения правовых данных
b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
a) Хищение жестких дисков, подключение к сети, инсайдерство
b) Перехват данных, хищение данных, изменение архитектуры системы
c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:
a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
a) несанкционированного доступа, воздействия в сети
b) инсайдерства в организации
c) чрезвычайных ситуаций

5. Основные объекты информационной безопасности:
a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:
a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:
a) Экономической эффективности системы безопасности
b) Многоплатформенной реализации системы
c) Усиления защищенности всех звеньев системы

8. Основными субъектами информационной безопасности являются:
a) руководители, менеджеры, администраторы компаний
b) органы права, государства, бизнеса
c) сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести все перечисленное:
a) Установление регламента, аудит системы, выявление рисков
b) Установка новых офисных приложений, смена хостинг-компании
c) Внедрение аутентификации, проверки контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:
a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности

11. Принципом политики информационной безопасности является принцип:
a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы

c) Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:

a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы

14. К основным типам средств воздействия на компьютерную сеть относится:

a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания

15. Когда получен спам по e-mail с приложенным файлом, следует:

a) Прочитать приложение, если оно не содержит ничего ценного – удалить
b) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:

a) Секретность ключа определена секретностью открытого сообщения
b) Секретность информации определена скоростью передачи данных
c) Секретность закрытого сообщения определяется секретностью ключа

17. ЭЦП – это:

a) Электронно-цифровой преобразователь
b) Электронно-цифровая подпись
c) Электронно-цифровой процессор

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:

a) Покупка нелицензионного ПО
b) Ошибки эксплуатации и неумышленного изменения режима работы системы
c) Сознательного внедрения сетевых вирусов

19. Наиболее распространены угрозы информационной безопасности сети:

a) Распределенный доступ клиент, отказ оборудования
b) Моральный износ сети, инсайдерство
c) Сбой (отказ) оборудования, нелегальное копирование данных

20. Наиболее распространены средства воздействия на сеть офиса:

a) Слабый трафик, информационный обман, вирусы в интернет
b) Вирусы в сети, логические мины (закладки), информационный перехват
c) Компьютерные сбои, изменение администрирования, топологии

21. Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальностьl

23. Угроза информационной системе (компьютерной сети) – это:

a) Вероятное событие
b) Детерминированное (всегда определенное) событие
c) Событие, происходящее периодически

24. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

a) Регламентированной
b) Правовой
c) Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

a) Программные, технические, организационные, технологические
b) Серверные, клиентские, спутниковые, наземные
c) Личные, корпоративные, социальные, национальные

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 навыков. 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 учебная литература:

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере: учебное пособие / А. Е. Фаронов. — 3-е изд. — 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
2. 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 учебная литература:

1. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / 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
2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. — Саратов: Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/72345.html
3. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/86938.html

8.3. Периодические издания:

1. Вестник Московского государственного технического университета имени Н.Э. Баумана. Серия Естественные науки. ISSN 1812-3368. https://www.iprbookshop.ru/23124.html
2. Информационные технологии моделирования и управления. ISSN 1813-9744. https://www.iprbookshop.ru/43350.html .
3. Журнал «Образование и Информатика». http://infojournal.ru

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

1. Федеральный портал «Российское образование». http://www.edu.ru/
2. Электронно-библиотечная система «Научная электронная библиотека eLIBRARY.RU» https://www.elibrary.ru /
4. Электронно-библиотечная система ЛАНЬ https://e.lanbook.com/
3. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru

4. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)
5. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
6. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
7. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)

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

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекций, семинарских 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:

1. Подготовка к экзамену (зачету) должна проводиться систематически, в течение всего семестра.
2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.
3. 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 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. Microsoft Windows Server;
2. Семейство ОС Microsoft Windows;
3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом;
4. Информационно-справочная система: Система КонсультантПлюс (КонсультантПлюс);
5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (Система ГАРАНТ);

Перечень используемого программного обеспечения указан в п.12 данной рабочей программы дисциплины.

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 (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя; компьютеры в сборе для обучающихся; наушники; телевизор.

Перечень лицензионного программного обеспечения, в том числе отечественного производства и свободно распространяемого программного обеспечения:

Windows Server 2016, Windows 10, Microsoft Office, КонсультантПлюс, Система ГАРАНТ, Kaspersky Endpoint Security, Microsoft Windows Server, Microsoft Project, Spider Project, EclipseIDEforJavaEEDevelopers, AndroidStudio, IntelliJIDEA, Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype, Gimp, Paint.net, AnyLogic, Inkscape, Microsoft Visual Studio Community, Denver, GNU Octave, PostgreSQL, Ramus.

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 (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя; компьютеры в сборе для обучающихся; колонки; проектор, экран.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows Server 2016, Windows 10, Microsoft Office, КонсультантПлюс, Система ГАРАНТ, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype, Zoom, Gimp, Paint.net, AnyLogic, Inkscape.

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;
- семинарские 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.