Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки	Бизнес-информатика
Код	38.03.05
Направленность(профиль)	Информационные системы и технологии в бизнесе
Квалификация выпускника	бакалавр

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01EB91710023B0C5B64D74F7781AC11FE2
Владелец: МАНЮШИС АЛЬГИРДАС ЮОЗО
Действителен: с 16.06.2023 до 16.09.2024

Москва
2024

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

Группа компетенций	Категория компетенций	Код
Общепрофессиональные		ОПК-3

2. Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-3	Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.1 Знает понятие, виды и особенности продуктов и услуг в сфере ИКТ; основы алгоритмизации, современные методологии разработки программных средств; этапы разработки программных средств; методы обеспечения информационной безопасности. ОПК-3.2 Умеет разрабатывать алгоритмы и программы для практической реализации продуктов и услуг в сфере ИКТ. ОПК-3.3 Владеет методами управления процессами создания и использования продуктов и услуг в сфере ИКТ, в частности, навыками разработки алгоритмов и программ для их практической реализации.

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	**ОПК-3**		
	роль и задачи информационной безопасности на предприятии; - техническое и программное обеспечение для решения задач	- формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и	навыками реализации мер по обеспечению ИБ с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий и

	информационной безопасности (ИБ); - методы и средства защиты информации; - вероятные угрозы ИБ.	технической реализуемости и экономической целесообразности; - использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в профессиональной деятельности.	вероятных угроз; - инструментальными средствами защиты информации; - навыками обеспечения целостности, доступности и конфиденциальности информации; - навыками работы по реализации политики информационной безопасности.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» учебного плана.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как «Информатика», «Технологии и методы программирования», «Технологии и методы программирования», «Компьютерная графика и мультимедиа», «Операционные системы».

Изучение дисциплины позволит обучающимся реализовывать компетенции в профессиональной деятельности.

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

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников.

5. Объем дисциплины

Виды учебной работы	***Формы обучения***
	очная форма
Общая трудоемкость: зачетные единицы/часы	2/72
Контактная работа:	
Занятия лекционного типа	18
Занятия семинарского типа	18
Промежуточная аттестация: **зачет**	0,1
Самостоятельная работа (СРС)	35,9

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)			
		Аудиторная работа			Самостоятельная работа
		ЛЗ	ПЗ	ЛабЗ	

1	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	2	2	-	5,9
2	Нормативно - законодательная база и стандарты в области информационной безопасности	2	2	-	6
3	Угрозы информационной безопасности, их классификация и анализ.	2	2	-	6
4	Методы и средства обеспечения информационной безопасности.	4	4	-	6
5	Информационная безопасность автоматизированных систем	4	4	-	6
6	Информационная безопасность компьютеров и компьютерных сетей	4	4	-	6
	Промежуточная аттестация	0,1			
	Итого	18	18	-	35,9

6.2. Программа дисциплины структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного курса
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. 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	Основные нормативно-справочные документы. Законодательная база информационной безопасности. 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	Организационно-административные, технические, криптографические методы защиты информации.

	информационной безопасности.	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	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.

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.	***Вопросы:*** 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	***Вопросы:*** 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.	***Вопросы:*** 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.	***Вопросы:*** 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	***Вопросы:*** 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	***Вопросы:*** 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	Формы и тематика самостоятельной работы
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	Первоочередные мероприятия по реализации государственной политики обеспечения Изучение информационных процессов. Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами
2.	Нормативно - законодательная база и стандарты в области информационной безопасности	Законодательный уровень информационной безопасности Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами
3.	Угрозы информационной безопасности, их классификация и анализ.	Классификация угроз Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
4.	Методы и средства обеспечения информационной безопасности.	Административный уровень информационной безопасности Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
5.	Информационная безопасность автоматизированных систем	Модели политик безопасности и их сравнение Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
6.	Информационная безопасность компьютеров и компьютерных сетей	Программно-технические средства защиты информации в ПК Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания

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)	Формы текущего контроля
1.	Основные понятия информационной	Вопросы к занятию, тестирование.

	безопасности и ее место в системе национальной безопасности РФ.	
2.	Нормативно - законодательная база и стандарты в области информационной безопасности	Вопросы к занятию, интерактивные занятия, тестирование.
3.	Угрозы информационной безопасности, их классификация и анализ.	Вопросы к занятию, практические задания, тестирование.
4.	Методы и средства обеспечения информационной безопасности.	Вопросы к занятию, практические задания, тестирование.
5.	Информационная безопасность автоматизированных систем	Вопросы к занятию, практические задания, информационные проекты, тестирование.
6.	Информационная безопасность компьютеров и компьютерных сетей	Вопросы к занятию, информационные проекты, тестирование.

7.2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе промежуточного контроля

Тема 1. Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.

Вопросы к занятию:

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.

Тема 2. Нормативно - законодательная база и стандарты в области информационной безопасности

Вопросы к занятию:

1. Что такое законодательный уровень информационной безопасности?
2. В чем состоит отличительная особенность стандарта шифрования AESot DES?
3. Что собой представляет конфиденциальная информация?
4. Что собой представляет электронная подпись?
5. Какие виды требований входят в «Общие критерии»?

Типовые задания к интерактивным занятиям

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

Тема 3. Угрозы информационной безопасности, их классификация и анализ

Вопросы к занятию:

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.

Практические задания

Задание № 1.

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

Задание № 2.

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

Задание № 3.

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 № 4.

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

Тема 4. Методы и средства обеспечения информационной безопасности.

Вопросы к занятию:

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.

Практические задания

Задание № 1.

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

Задание № 2.

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

Задание № 3.

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

Тема 5. Информационная безопасность автоматизированных систем

Вопросы к занятию:

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 систем

Примерная тематика презентаций (информационных проектов)

1. Основные задачи и проблемы информационной безопасности
2. Киберпреступность
3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.
4. Угрозы информационной безопасности и управление рисками.
5. Причины, виды, каналы утечки и искажения информации.
6. Технические каналы утечки информации.
7. Технические средства обеспечения безопасности объекта.
8. Программно-аппаратные средства обеспечения информационной безопасности.
9. Методы контроля доступа к информации.
10. Вредоносные программы.

Практические задания

Задание № 1.

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 № 1.

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

Задание № 3.

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

Тема 6. Информационная безопасность компьютеров и компьютерных сетей

Вопросы к занятию:

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.

Примерная тематика презентаций (информационных проектов)

1. Основы криптографической защиты информации.
2. Обеспечение информационной безопасности операционных систем
3. Основы безопасности сетевых технологий.
4. Организационно-правовое обеспечение защиты информации.
5. Стандарты информационной безопасности
6. Информация как наиболее ценный ресурс современного общества.
7. Актуальность и значимость информационной безопасности.
8. Государственная информационная политика РФ.

Типовые тестовые вопросы для промежуточной аттестации

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 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. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 c. — 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. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : Евразийский открытый институт, 2010. — 328 c. — ISBN 978-5-374-00381-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10746.html

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

4. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 c. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133957.html

8.2.Дополнительная учебная литература:

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 c.— Режим доступа: http://www.iprbookshop.ru/33857

2. 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 c.— Режим доступа: http://www.iprbookshop.ru/57143

3. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430

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. Федеральный портал «Российское образование». http://www.edu.ru/
2. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru /

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

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекционных занятий, 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:

- работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
- внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
- выполнение самостоятельных практических работ;
- 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 с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение различных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии.

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 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. 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 образовательной программой, 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 – лекционные занятия (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация) и практические занятия, так и активные и интерактивные формы занятий - диспуты, решение ситуационных задач, ролевые игры и разбор конкретных ситуаций.

На учебных занятиях используются технические средства обучения – проектор, ноутбук, проекционный экран, колонки 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;
- контрольные опросы;
- консультации;
- самостоятельная работа с учебной литературой;
- подготовка и обсуждение рефератов, презентаций;
- 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:

- *анализ проблемных-аналитических заданий,*
- *творческие задания;*
- *дискуссия.*

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.

Приложение

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ДИСЦИПЛИНЕ

Информационная безопасность

Направление подготовки	Бизнес-информатика
Код	38.03.05
Направленность (профиль)	Информационные системы и технологии в бизнесе
Квалификация выпускника	бакалавр

Москва
2024

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

Группа компетенций	Категория компетенций	Код
Общепрофессиональные		ОПК-3

2. Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-3	Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.1 Знает понятие, виды и особенности продуктов и услуг в сфере ИКТ; основы алгоритмизации, современные методологии разработки программных средств; этапы разработки программных средств; методы обеспечения информационной безопасности. ОПК-3.2 Умеет разрабатывать алгоритмы и программы для практической реализации продуктов и услуг в сфере ИКТ. ОПК-3.3 Владеет методами управления процессами создания и использования продуктов и услуг в сфере ИКТ, в частности, навыками разработки алгоритмов и программ для их практической реализации.

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	ОПК-3		
	роль и задачи информационной безопасности на предприятии; - техническое и программное обеспечение для решения задач	- формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической	навыками реализации мер по обеспечению ИБ с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий и вероятных угроз;

	информационной безопасности (ИБ); - методы и средства защиты информации; - вероятные угрозы ИБ.	реализуемости и экономической целесообразности; - использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в профессиональной деятельности.	- инструментальными средствами защиты информации; - навыками обеспечения целостности, доступности и конфиденциальности информации; - навыками работы по реализации политики информационной безопасности.

3.2.Критерии оценки результатов обучения по дисциплине

Шкала оценивания	**Индикаторы достижения**	**Показатели оценивания результатов обучения**
ОТЛИЧНО/ЗАЧТЕНО	Знает:	- студент глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- студент умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.
	Владеет:	- студент владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО/ЗАЧТЕНО	Знает:	- студент твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- студент умеет самостоятельно и в основном правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя

		научные понятия и ссылки на нормативную базу.
	Владеет:	- студент в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
УДОВЛЕТВОРИТЕЛЬНО/ЗАЧТЕНО	Знает:	- студент ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- студент в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- студент владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
Компетенция не достигнута		
НЕУДОВЛЕТВОРИТЕЛЬНО/ НЕЗАЧТЕНО	Знает:	- студент не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.
	Умеет:	студент не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым “удовлетворительно”.

4. Типовые контрольные задания и/или иные материалы для проведения промежуточной аттестации, необходимые для оценки знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

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

11. Классификация компьютерных вирусов
1) по деструктивным возможностям
2) по размеру
3) по среде обитания
4) по особенностям алгоритма
5) по способу заражения

12. К методам защиты от НСД относятся
1) уменьшение доступа;
2) разграничение доступа;
3) увеличение доступа;
4) приостановка доступа;
5) аутентификация и идентификация

13. Совокупность правил, процедур, принципов в области ИБ, которыми руководствуется организация в своей деятельности называется
1) политикой информации
2) защитой информации
3) политикой безопасности
4) организацией безопасности

14. Как подразделяются вирусы в зависимости от деструктивных возможностей?
1) Сетевые, файловые, загрузочные,
2) Безвредные, неопасные, опасные,
3) Резидентные, нерезидентные
4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические"

15. Причины возникновения ошибок в данных
1) Погрешность измерений
2) Неверная интерпретация данных
3) Ошибки при переносе данных с промежуточного документа в компьютер

4) Использование недопустимых методов анализа данных
5) Преднамеренное искажение данных

16. Наиболее эффективное средство для защиты от сетевых атак
1) использование сетевых экранов
2) использование антивирусных программ
3) посещение только «надёжных» Интернет-источников
4) использование только сертифици-рованных программ

17. Простейший способ идентификации в КС:
1) Токен
2) Password
3) Пароль
4) Login
5) Смарт-карта

18. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами:
1) Антивирус
2) Замок
3) Брандма́уэр
4) Криптография
5) Экспертная система

19. Хищение информации – это…
1) Несанкционированное копирование информации
2) Утрата информации
3) Блокирование информации
4) Искажение информации
5) Продажа информации

20. Троянские программы бывают:
1) утилиты удалённого администрирования
2) программы - шпионы
3) рекламные программы
4) программы удаления данных на локальном компьютере

21. Сетевые черви бывают:
1) Web-черви
2) почтовые черви
3) черви операционной системы
4) черви MS Office

22. К биометрическим системам защиты информации относятся системы идентификации по:
1) отпечаткам пальцев
2) радужной оболочке глаза
3) росту
4) весу
5) цвету глаз
6) характеристикам речи

23. Достоинства симметричных ключей
1) Высокая скорость шифрования
2) Низкая скорость шифрования
3) Меньшая длина ключей
4) Большая длина ключей
5) Простота реализации

24. Формой правовой защиты литературных, художественных и научных произведений является (...) право
1) литературное
2) художественное
3) авторское
4) патентное

Вопросы к промежуточной аттестации

1. Значение информации и ее защиты.
2. Информационная безопасность и защита информации.
3. Составляющие ИБ: доступность, целостность, конфиденциальность.
4. Основные понятия в области ИБ.
5. Нарушители ИБ.
6. Объекты защиты информации. Виды информации в области ЗИ.
7. Коммерческая тайна.
8. Уровни формирования ИБ.
9. Причины уязвимости компьютерных систем.
10. Классификация средств защиты в компьютерных сетях
11. Методы и средства защиты информации.
12. Законодательно-правовой уровень ЗИ.
13. Ответственность за нарушения в сфере ИБ.
14. Административный уровень обеспечения ИБ. Политика ИБ.
15. Авторское и патентное право
16. Программно-технический уровень ЗИ.
17. Идентификация и аутентификация
18. Управление доступом
19. Регистрация и аудит
20. Криптография. Симметричные криптосистемы.
21. Симметричные шифры
22. Криптография. Асимметричные криптосистемы.
23. Электронно-цифровая подпись.
24. Организационное обеспечение ЭЦП. Две модели сертификации
25. Аппаратные и программные брандмауэры.
26. Анализ защищенности
27. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры
28. Компьютерные вирусы
29. Технологии обнаружения вирусов. Антивирусные средства.
30. Стандарты в области информационной безопасности.

Примеры проблемно-аналитических заданий

1. Проанализируйте отличия понятий «информационная безопасность» и «защита информации».
2. Сделайте анализ причин уязвимости компьютерных систем.

3. В чем заключаются отличия авторского и патентного прав?
4. Обсудите механизмы обеспечения невозможности отказа от авторства
5. Анализ влияния процессов информатизации общества на составляющие национальной безопасности и их содержание.
6. Разработайте модель нарушителя информационных систем
7. Проведите сравнительный анализ моделей политик безопасности.

Практические работы

1. Изучение положений о государственном лицензировании деятельности в области защиты информации
2. Система сертификации средств криптографической защиты информации
3. Изучение положения о сертификации средств вычислительной техники и связи
4. Особенности подготовки, и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. Изучение особенностей аттестации помещений по требованиям безопасности информации
7. Анализ рисков информационной безопасности
8. Обеспечение информационной безопасности в ведущих зарубежных странах
9. Построение концепции информационной безопасности предприятия
10. Процедура аутентификации пользователя на основе пароля
11. Программная реализация криптографических алгоритмов
12. Механизмы контроля целостности данных
13. Алгоритмы поведения вирусных и других вредоносных программ
14. Алгоритмы предупреждения и обнаружения вирусных угроз
15. Пакеты антивирусных программ»

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

Специфика формирования компетенций и их измерение определяется структурированием информации о состоянии уровня подготовки обучающихся.

Алгоритмы отбора и конструирования заданий для оценки достижений в предметной области, техника конструирования заданий, способы организации и проведения стандартизированный оценочных процедур, методика шкалирования и методы обработки и интерпретации результатов оценивания позволяют обучающимся освоить компетентностно-ориентированные программы дисциплин.

Формирование компетенций осуществляется в ходе всех видов занятий, практики, а контроль их сформированности на этапе текущей, промежуточной и итоговой аттестации.

Оценивание знаний, умений и навыков по учебной дисциплине осуществляется посредством использования следующих видов оценочных средств:

- опросы: устный, письменный;
- задания для практических занятий;
- ситуационные задания;
- контрольные работы;
- коллоквиумы;
-написание реферата;
-написание эссе;
- решение тестовых заданий;

- экзамен.

Опросы по вынесенным на обсуждение темам

Устные опросы проводятся во время практических занятий и возможны при проведении аттестации в качестве дополнительного испытания при недостаточности результатов тестирования и решения заданий. Вопросы опроса не должны выходить за рамки объявленной для данного занятия темы. Устные опросы необходимо строить так, чтобы вовлечь в тему обсуждения максимальное количество обучающихся в группе, проводить параллели с уже пройденным учебным материалом данной дисциплины и смежными курсами, находить удачные примеры из современной действительности, что увеличивает эффективность усвоения материала на ассоциациях.

Основные вопросы для устного опроса доводятся до сведения студентов на предыдущем практическом занятии.

Письменные опросы позволяют проверить уровень подготовки к практическому занятию всех обучающихся в группе, при этом оставляя достаточно учебного времени для иных форм педагогической деятельности в рамках данного занятия. Письменный опрос проводится без предупреждения, что стимулирует обучающихся к систематической подготовке к занятиям. Вопросы для опроса готовятся заранее, формулируются узко, дабы обучающийся имел объективную возможность полноценно его осветить за отведенное время.

Письменные опросы целесообразно применять в целях проверки усвояемости значительного объема учебного материала, например, во время проведения аттестации, когда необходимо проверить знания, обучающихся по всему курсу.

При оценке опросов анализу подлежит точность формулировок, связность изложения материала, обоснованность суждений.

Решение заданий (кейс-методы)

Решение кейс-методов осуществляется с целью проверки уровня навыков (владений) обучающегося по применению содержания основных понятий и терминов дисциплины вообще и каждой её темы в частности.

Обучающемуся объявляется условие задания, решение которого он излагает либо устно, либо письменно.

Эффективным интерактивным способом решения задания является сопоставления результатов разрешения одного задания двумя и более малыми группами обучающихся.

Задачи, требующие изучения значительного объема, необходимо относить на самостоятельную работу студентов, с непременным разбором результатов во время практических занятий. В данном случае решение ситуационных задач с глубоким обоснованием должно представляться на проверку в письменном виде.

При оценке решения заданий анализируется понимание обучающимся конкретной ситуации, правильность её понимания в соответствии с изучаемым материалом, способность обоснования выбранной точки зрения, глубина проработки рассматриваемого вопроса, умением выявить основные положения затронутого вопроса.

Решение заданий в тестовой форме

Проводится тестирование в течение изучения дисциплины

Не менее чем за 1 неделю до тестирования, преподаватель должен определить обучающимся исходные данные для подготовки к тестированию: назвать разделы (темы, вопросы), по которым будут задания в тестовой форме, теоретические источники (с точным указанием разделов, тем, статей) для подготовки.

При прохождении тестирования пользоваться конспектами лекций, учебниками, и иными материалами не разрешено.