Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Основы информационной безопасности

Направление подготовки	Инноватика
Код	27.03.05
Направленность (профиль)	Инновационный менеджмент
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	**Категория компетенций**	**Код**
Общепрофессиональные	Использование компьютерных технологий	ОПК-7

2. **Компетенции и индикаторы их достижения**

Код компетенции	**Формулировка компетенции**	**Индикаторы достижения компетенции**
ОПК-7	Способен использовать информационно-коммуникационные компьютерные технологии, базы данных, пакеты прикладных программ для решения инженерно-технических и технико-экономических задач планирования и управления работами по инновационным проектам	ОПК-7.1. Знает основы и принципы работы информационных технологий ОПК-7.2. Умеет выполнять практические работы по настройке компьютерной техники, использовать современных информационные технологии и программное обеспечение для решения задач профессиональной деятельности ОПК-7.3. Владеет навыками работы с прикладным программным обеспечением

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

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	**Знать**	**Уметь**	**Владеть**
Код компетенции	ОПК-7		
	принципы и методы, средства решения задач с учетом основных требований информационной безопасности	решать задачи профессиональной деятельности на основе информационной культуры и с учетом информационной безопасности	навыками работы с программным обеспечением, соблюдая требования информационной безопасности

4. **Место дисциплины (модуля) в структуре образовательной программы**

Дисциплина относится к обязательной части учебного плана образовательной программы. Данная дисциплина взаимосвязана с другими дисциплинами ОПОП.

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

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

5. Объем дисциплины

Виды учебной работы	***Форма обучения***
	Очная
Общая трудоемкость: зачетные единицы/часы	4/144
Контактная работа:	
Занятия лекционного типа	36
Занятия семинарского типа	36
Промежуточная аттестация: **зачет с оценкой**	0,15
Самостоятельная работа (СРС)	71,85

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.	Основы информационной безопасности	2		2				5,85
2.	Защищаемая информация	4		4				6
3.	Классификация автоматизированных систем	2		2				7
4.	Классы защищённости автоматизированных систем	4		4				7
5.	Угрозы и уязвимости информационной	4		4				7

	безопасности							
6.	Технические каналы утечки информации	4		4				7
7.	Угрозы несанкционированного доступа к информации	4		4				8
8.	Правовой уровень обеспечения информационной безопасности	4		4				8
9.	Основные понятия криптографии	4		4				8
10.	Алгоритмы цифровой подписи	4		4				8
	Итого	36		36				71,85

6.2.Программа дисциплины, структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1.	Основы информационной безопасности	Основные понятия, термины и определения в области информационной безопасности. Механизмы обеспечения Безопасности. Актив. Критерии информационной безопасности. Информация, виды информации. Контроль доступа. Защищаемые помещения. Классификационная схема понятий в области «Защита информации»
2.	Защищаемая информация	Общедоступная информация. Информация ограниченного доступа. Персональные данные. Категории обрабатываемых персональных данных (ПДн). Государственная тайна. Служебная тайна. Коммерческая тайна
3.	Классификация автоматизированных систем	Автоматизированная система. Информационная система персональных данных (ИСПДн). Государственные информационные системы (ГИС). Информационные системы общего пользования (ИСОП). Режимы обработки данных в АС. Определяющие признаки при классификации АС. Классификация автоматизированных систем
4.	Классы защищённости автоматизированных систем	Уровни защищенности персональных данных. Угрозы безопасности ПДн. Уровни защищенности ИСПДн. Класс защищённости ГИС не составляющей государственную тайну. Степени возможного ущерба от нарушения свойств безопасности информации. Класс защищённости ГИС.
5.	Угрозы и уязвимости информационной безопасности	Общая классификация угроз и уязвимостей информационных систем. Структура угроз. Составляющие угрозы. Уязвимость. Факторы, воздействующие на информацию. Объективные внутренние факторы. Объективные внешние факторы.

		Субъективные внутренние факторы. Субъективные внешние факторы. Обобщенная модель способов овладения конфиденциальной информацией.
6.	Технические каналы утечки информации	Технический канал утечки информации. Описание угрозы утечки информации по ТКУИ. Источники угроз утечки информации по ТКУИ. Среда распространения информативного сигнала. Источники (носители) информации. Технические каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки информации, обрабатываемой ТСПИ. Технические каналы утечки видовой информации
7.	Угрозы несанкционированного доступа к информации	Угрозы НСД (несанкционированные действия). Угрозы непосредственного доступа. Угрозы удаленного доступа. Варианты описания угроз НСД. Источники угроз НСД. Типы нарушителей. Категории внутренних нарушителей. Источники угроз НСД. Основные группы уязвимостей ИС. Причины возникновения уязвимостей. Классификация уязвимостей программного обеспечения. Уязвимости системного ПО. Уязвимости протоколов сетевого взаимодействия. Классификация угроз по условиям реализации. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Анализ сетевого трафика. Сканирование сети. Угроза выявления пароля. Отказ в обслуживании. DDoS-атаки.
8.	Правовой уровень обеспечения информационной безопасности	Международные и российские стандарты в области информационной безопасности. Нормативно-правовые и руководящие документы ФСТЭКа РФ по защите информации от несанкционированного доступа (НСД) к информационным системам. 149-ФЗ «Об информации, информационных технологиях и о защите информации». 152-ФЗ «О персональных данных». 98-ФЗ «О коммерческой тайне». 63-ФЗ «Об электронной подписи» 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
9.	Основные понятия криптографии	Место криптографии среди других наук. Классификация методов преобразования информации. Основные понятия и определения. Смежные дисциплины. История криптографии
10.	Алгоритмы цифровой подписи	Цифровая подпись. Требования к цифровой подписи. Алгоритмы асимметричного шифрования (цифровой подписи). Стандарт цифровой подписи DSS. Алгоритм цифровой подписи ECDSA. ГОСТ 34.10-2018 «Процессы формирования и проверки электронной цифровой подписи». Использование цифровой подписи

6.2.2. Содержание практических занятий

№	Наименование темы	Содержание практического занятия

п/п	(раздела) дисциплины	
1.	Основы информационной безопасности	Основные понятия, термины и определения в области информационной безопасности. Механизмы обеспечения Безопасности. Актив. Критерии информационной безопасности. Информация, виды информации. Контроль доступа. Защищаемые помещения. Классификационная схема понятий в области «Защита информации»
2.	Защищаемая информация	Общедоступная информация. Информация ограниченного доступа. Персональные данные. Категории обрабатываемых персональных данных (ПДн). Государственная тайна. Служебная тайна. Коммерческая тайна
3.	Классификация автоматизированных систем	Автоматизированная система. Информационная система персональных данных (ИСПДн). Государственные информационные системы (ГИС). Информационные системы общего пользования (ИСОП). Режимы обработки данных в АС. Определяющие признаки при классификации АС. Классификация автоматизированных систем
4.	Классы защищённости автоматизированных систем	Уровни защищенности персональных данных. Угрозы безопасности ПДн. Уровни защищенности ИСПДн. Класс защищённости ГИС не составляющей государственную тайну. Степени возможного ущерба от нарушения свойств безопасности информации. Класс защищённости ГИС.
5.	Угрозы и уязвимости информационной безопасности	Общая классификация угроз и уязвимостей информационных систем. Структура угроз. Составляющие угрозы. Уязвимость. Факторы, воздействующие на информацию. Объективные внутренние факторы. Объективные внешние факторы. Субъективные внутренние факторы. Субъективные внешние факторы. Обобщенная модель способов овладения конфиденциальной информацией.
6.	Технические каналы утечки информации	Технический канал утечки информации. Описание угрозы утечки информации по ТКУИ. Источники угроз утечки информации по ТКУИ. Среда распространения информативного сигнала. Источники (носители) информации. Технические каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки информации, обрабатываемой ТСПИ. Технические каналы утечки видовой информации
7.	Угрозы несанкционированного доступа к информации	Угрозы НСД (несанкционированные действия). Угрозы непосредственного доступа. Угрозы удаленного доступа. Варианты описания угроз НСД. Источники угроз НСД. Типы нарушителей. Категории внутренних нарушителей. Источники угроз НСД. Основные группы уязвимостей ИС. Причины возникновения уязвимостей. Классификация уязвимостей программного обеспечения. Уязвимости системного ПО. Уязвимости

		протоколов сетевого взаимодействия. Классификация угроз по условиям реализации. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Анализ сетевого трафика. Сканирование сети. Угроза выявления пароля. Отказ в обслуживании. DDoS-атаки.
8.	Правовой уровень обеспечения информационной безопасности	Международные и российские стандарты в области информационной безопасности. Нормативно-правовые и руководящие документы ФСТЭКа РФ по защите информации от несанкционированного доступа (НСД) к информационным системам. 149-ФЗ «Об информации, информационных технологиях и о защите информации». 152-ФЗ «О персональных данных». 98-ФЗ «О коммерческой тайне». 63-ФЗ «Об электронной подписи» 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
9.	Основные понятия криптографии	Место криптографии среди других наук. Классификация методов преобразования информации. Основные понятия и определения. Смежные дисциплины. История криптографии
10.	Алгоритмы цифровой подписи	Цифровая подпись. Требования к цифровой подписи. Алгоритмы асимметричного шифрования (цифровой подписи). Стандарт цифровой подписи DSS. Алгоритм цифровой подписи ECDSA. ГОСТ 34.10-2018 «Процессы формирования и проверки электронной цифровой подписи». Использование цифровой подписи

6.2.3. Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание самостоятельной работы
1.	Основы информационной безопасности	Основные понятия, термины и определения в области информационной безопасности. Механизмы обеспечения Безопасности. Актив. Критерии информационной безопасности. Информация, виды информации. Контроль доступа. Защищаемые помещения. Классификационная схема понятий в области «Защита информации»
2.	Защищаемая информация	Общедоступная информация. Информация ограниченного доступа. Персональные данные. Категории обрабатываемых персональных данных (ПДн). Государственная тайна. Служебная тайна. Коммерческая тайна
3.	Классификация автоматизированных систем	Автоматизированная система. Информационная система персональных данных (ИСПДн). Государственные информационные системы (ГИС). Информационные системы общего пользования (ИСОП). Режимы обработки данных в АС. Определяющие признаки при классификации АС. Классификация автоматизированных систем

4.	Классы защищённости автоматизированных систем	Уровни защищенности персональных данных. Угрозы безопасности ПДн. Уровни защищенности ИСПДн. Класс защищённости ГИС не составляющей государственную тайну. Степени возможного ущерба от нарушения свойств безопасности информации. Класс защищённости ГИС.
5.	Угрозы и уязвимости информационной безопасности	Общая классификация угроз и уязвимостей информационных систем. Структура угроз. Составляющие угрозы. Уязвимость. Факторы, воздействующие на информацию. Объективные внутренние факторы. Объективные внешние факторы. Субъективные внутренние факторы. Субъективные внешние факторы. Обобщенная модель способов овладения конфиденциальной информацией.
6.	Технические каналы утечки информации	Технический канал утечки информации. Описание угрозы утечки информации по ТКУИ. Источники угроз утечки информации по ТКУИ. Среда распространения информативного сигнала. Источники (носители) информации. Технические каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки информации, обрабатываемой ТСПИ. Технические каналы утечки видовой информации
7.	Угрозы несанкционированного доступа к информации	Угрозы НСД (несанкционированные действия). Угрозы непосредственного доступа. Угрозы удаленного доступа. Варианты описания угроз НСД. Источники угроз НСД. Типы нарушителей. Категории внутренних нарушителей. Источники угроз НСД. Основные группы уязвимостей ИС. Причины возникновения уязвимостей. Классификация уязвимостей программного обеспечения. Уязвимости системного ПО. Уязвимости протоколов сетевого взаимодействия. Классификация угроз по условиям реализации. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Анализ сетевого трафика. Сканирование сети. Угроза выявления пароля. Отказ в обслуживании. DDoS-атаки.
8.	Правовой уровень обеспечения информационной безопасности	Международные и российские стандарты в области информационной безопасности. Нормативно-правовые и руководящие документы ФСТЭКа РФ по защите информации от несанкционированного доступа (НСД) к информационным системам. 149-ФЗ «Об информации, информационных технологиях и о защите информации». 152-ФЗ «О персональных данных». 98-ФЗ «О коммерческой тайне». 63-ФЗ «Об электронной подписи» 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
9.	Основные понятия криптографии	Место криптографии среди других наук. Классификация методов преобразования информации. Основные понятия и определения. Смежные

		дисциплины. История криптографии
10.	Алгоритмы цифровой подписи	Цифровая подпись. Требования к цифровой подписи. Алгоритмы асимметричного шифрования (цифровой подписи). Стандарт цифровой подписи DSS. Алгоритм цифровой подписи ECDSA. ГОСТ 34.10-2018 «Процессы формирования и проверки электронной цифровой подписи». Использование цифровой подписи

7. Текущий контроль по дисциплине (модулю) в рамках учебных занятий

В рамках текущего контроля преподаватель самостоятельно может проводить следующие мероприятия:

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Основы информационной безопасности	Опрос, практические задания, тестирование
2.	Защищаемая информация	Опрос, практические задания, тестирование
3.	Классификация автоматизированных систем	Опрос, практические задания, тестирование
4.	Классы защищённости автоматизированных систем	Опрос, практические задания, тестирование
5.	Угрозы и уязвимости информационной безопасности	Опрос, практические задания, тестирование
6.	Технические каналы утечки информации	Опрос, практические задания, тестирование
7.	Угрозы несанкционированного доступа к информации	Опрос, практические задания, тестирование
8.	Правовой уровень обеспечения информационной безопасности	Опрос, практические задания, тестирование
9.	Основные понятия криптографии	Опрос, практические задания, тестирование
10.	Алгоритмы цифровой подписи	Опрос, практические задания, тестирование

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

8.1. Основная учебная литература

1. Сидоренко, В. Г. Аспекты информационной безопасности : учебное пособие / В. Г. Сидоренко, Н. Н. Скоробогатова. — Москва : Российский университет транспорта (МИИТ), 2018. — 64 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115921.html

2. Информационная безопасность : учебное пособие / И. Б. Тесленко, Д. В. Виноградов, А. М. Губернаторов [и др.] ; под редакцией И. Б. Тесленко. — Владимир : Издательство Владимирского государственного университета, 2023. — 212 с. — ISBN 978-5-9984-1783-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/143816.html

3. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 282 с. — ISBN 978-5-4497-2420-5. — Текст : электронный // Цифровой

образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133959.html

8.2. Дополнительная учебная литература:

1. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108227.html

1. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146352.html

Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html

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. Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) https://www.elibrary.ru/defaultx.asp
3. https://www.rsl.ru/ Российская Государственная Библиотека (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:

- 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 (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. Терминальный сервер, предоставляющий к нему доступ клиентам на базе Windows Server 2016

2. Семейство ОС Microsoft Windows

3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом

4. Информационно-справочная система: Система КонсультантПлюс (Информационный комплекс)

5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (ЭПС «Система ГАРАНТ»)

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, оснащенная оборудованием и техническими средствами обучения.

Специализированная мебель:

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

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:

Операционные системы семейства Windows, КонсультантПлюс веб версия, Гарант веб версия, антивирус Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:
Яндекс Браузер, LibreOffice, МТС Линк, Notepad++. Pinta, Gimp, AnyLogic, Inkscape, OpenShot. FreeCAD, LibreCAD, Jamovi, Visual Studio, Unity.

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; доска (маркерная), комплект мебели для преподавателя.

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:
Операционные системы семейства Windows, КонсультантПлюс веб версия, Гарант веб версия, антивирус Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:
Яндекс Браузер, LibreOffice, МТС Линк, Notepad++. Pinta, Gimp, AnyLogic, Inkscape, OpenShot. FreeCAD, LibreCAD, Jamovi, Visual Studio, Unity.

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.

Приложение

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Основы информационной безопасности

Направление подготовки	Инноватика
Код	27.03.05
Направленность (профиль)	Инновационный менеджмент
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Общепрофессиональные	Использование компьютерных технологий	ОПК-7

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ОПК-7	Способен использовать информационно-коммуникационные компьютерные технологии, базы данных, пакеты прикладных программ для решения инженерно-технических и технико-экономических задач планирования и управления работами по инновационным проектам	ОПК-7.1. Знает основы и принципы работы информационных технологий ОПК-7.2. Умеет выполнять практические работы по настройке компьютерной техники, использовать современных информационные технологии и программное обеспечение для решения задач профессиональной деятельности ОПК-7.3. Владеет навыками работы с прикладным программным обеспечением

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

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	ОПК-7		
	принципы и методы, средства решения задач с учетом основных требований информационной безопасности	решать задачи профессиональной деятельности на основе информационной культуры и с учетом информационной безопасности	навыками работы с программным обеспечением, соблюдая требования информационной безопасности

3.2. Критерии оценки результатов обучения по дисциплине

Шкала оценивания	Индикаторы достижени	Показатели оценивания результатов обучения

	я	
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/ НЕ ЗАЧТЕНО	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 достижения компетенции

ОПК-7

Тестирование

Вопрос №1. «Информационная система» это

Варианты ответов:

1. совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему
2. совокупность информации, технических средств и персонала, обслуживающего информационную систему
3. совокупность информации, информационных технологий и технических средств
4. совокупность информации, информационных технологий, технических средств и

персонала, обслуживающего систему
5. совокупность информационных технологий и технических средств

Вопрос №2. Выберите несколько значений/ К рекомендуемым методам и способам защиты информации в информационных системах относятся:
Тип ответа: Многие из многих
Варианты ответов:
1. методы и способы защиты информации от утечки по техническим каналам
2. методы и способы сокрытия информации от внутренних нарушителей
3. методы и способы защиты информации от несанкционированного доступа
4. методы и способы устранения конкурентов

Вопрос №3. К основным видам политики безопасности не относится следующая:
Варианты ответов:
1. дискреционная
2. матричная (двухмерная)
3. трехмерная
4. избирательная

Вопрос №4. Что понимается под использованием различных средств и методов, принятием мер и осуществлением мероприятий с целью системного обеспечения надежности передаваемой, хранимой и обрабатываемой информации?
Варианты ответов:
1. Защита информации
2. Сбор информации
3. Архивации информации;
4. Обработка информации
5. Проверка на вирус информации

Вопрос №5. Что из перечисленного относится к злоумышленным (преднамеренным угрозам)?
Варианты ответов:
1. Внедрение компьютерного вируса
2. Алгоритмические и программные ошибки
3. Ошибки человека при работе с ПК
4. Отказы и сбои аппаратуры в случае ее некачественного исполнения и физического старения
5. Помехи в каналах и на линиях связи от воздействия внешней среды

Тематика рефератов

1. Ценность информации. Цена информации.
2. Количество и качество информации.
3. Виды защищаемой информации.
4. Виды угроз безопасности информации.
5. Цели и задачи защиты информации.
6. Проблемы защиты информации.
7. Функциональное, организационное и структурное построение систем защиты информации.
8. Стандартизация систем защиты. Современные факторы, влияющие на защиту информации
9. Направления, виды и особенности деятельности спецслужб по

несанкционированному доступу к конфиденциальной информации.

10. Классификация информации. Виды данных и носителей.

Практические задания

Задание:

На основе анализа определений различных понятий, относящихся к данной предметной области, сформулировать определение понятия «чрезвычайная ситуация» в отношении процессов защиты информации;

Определить критерии, по которым можно провести классификацию потенциально возможных чрезвычайных ситуаций, способных влиять на функционирование комплексной системы защиты информации;

Изучить предлагаемую статью, посвященную вопросам разработки программы действий в чрезвычайных ситуациях на примере банка, и самостоятельно сформировать:

а) структуру паспорта риска объекта;

б) структуру группы (комитета) по управлению в условиях ЧС и ликвидации их последствий.

Перечень определений различных понятий, относящихся к категории экстремальных (чрезвычайных) событий:

Авария — опасное происшествие на хозяйствующем субъекте, транспорте или на линиях связи, представляющее угрозу жизни и здоровью людей либо приводящее к разрушению производственных помещений, повреждению или уничтожению оборудования, механизмов, транспортных средств, сырья и готовой продукции, а также к нарушению производственного процесса.

Катастрофа — внезапное бедствие, событие, влекущее за собой тяжелые последствия.

Кризисная ситуация — резкий, крутой перелом в чем-либо, тяжелое переходное состояние.

Риск — тип реализации опасностей определенного класса, который может быть определен как частота или как вероятность возникновения одного события при наступлении другого события.

Чрезвычайная ситуация — комплекс событий, протекание и результат наступления которых приводит к реализации в районе чрезвычайной ситуации, опасной для жизни и здоровья людей, а также материальных ценностей, нарушение экономической деятельности, нормального жизнеобеспечения, функционирования схем управления и связи, а также экологического равновесия.

Задания открытого типа

1. Конфиденциальность информации.
2. Целостность информации
3. Персональные данные.
4. Категории обрабатываемых персональных данных.
5. Государственная тайна.
6. Служебная тайна.
7. Информационные системы общего пользования (ИСОП).
8. Уровни защищенности персональных данных.
9. Классификация угроз.
10. Факторы, воздействующие на информацию.
11. Технический канал утечки информации.
12. Классификация угроз по условиям реализации
13. Вредоносные программы.

14. Определение возможных негативных последствий от реализации угроз безопасности информации.
15. Технические каналы утечки видовой информации
16. Коммерческая тайна.

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

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.