Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки Экономика

Код 38.03.01

Направленность (профиль) Экономика предприятий и организаций

Квалификация выпускника бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные компетенции	-	ПК-19

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-19	Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	ПК-19.1 Применяет в профессиональной деятельности современные методики анализа и оценки рисков ПК-19.3 Владеет конкретными способами предупреждения рисков и управления рисками в организации

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-19**		
Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	– содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей;	– применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий.	– основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером; – основными понятиями и методами информационной безопасности

4. Место дисциплины (модуля) в структуре образовательной программы

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

Данная дисциплина взаимосвязана с другими дисциплинами: «Информационные технологии в экономике», «Электронный бизнес и Интернет-технологии».

В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов: аналитической, организационно-управленческой, расчетно-экономической.

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: Экономика предприятий и организаций.

5. Объем дисциплины

Виды учебной работы	***Формы обучения***	
	Очная	***Очно-заочная с применением ДОТ***
Общая трудоемкость: зачетные единицы/часы	2/72	2/72
Контактная работа:		
Занятия лекционного типа	18	2
Занятия семинарского типа	18	4
Промежуточная аттестация: **зачет**	0,1	0,1
Самостоятельная работа (СРС)	35,9	65,9

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

6.1. Распределение часов по разделам/темам и видам работы

6.1.1. Очная форма обучения

№ п/п	**Раздел/тема**	**Виды учебной работы (в часах)**						
		Контактная работа						**Самостоятельная работа**
		Занятия лекционного типа		**Занятия семинарского типа**				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1.	Основы информационной безопасности.	2		2				3,9
2.	Нормативно-правовое регулирование ИБ в РФ и мире	2		2				4
3.	Угрозы и риски в цифровой экономике: виды и методы противодействия.	2		2				4
4.	Защита персональных данных и коммерческой тайны	2		2				4
5.	Кибербезопасность критически важной информационной инфраструктуры	2		2				4

	(КИИ)							
6.	Криптографические методы защиты информации	2		2				4
7.	Безопасность облачных сервисов и распределённых систем	2		2				4
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR	2		2				4
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия	2		2				4
	Промежуточная аттестация	**0,1**						
	Итого:	**18**		**18**				**35,9**
	Всего:	**72**						

6.1.3 Очно-заочная форма обучения с применением ДОТ

№ 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.							6
2.	Нормативно-правовое регулирование ИБ в РФ и мире	1						6
3.	Угрозы и риски в цифровой экономике: виды и методы противодействия.							8
4.	Защита персональных данных и коммерческой тайны	1						8
5.	Кибербезопасность критически важной информационной инфраструктуры (КИИ)							8
	Криптографические			1				8

6.	методы защиты информации							
7.	Безопасность облачных сервисов и распределённых систем			1				8
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR			1				7
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия			1				6,9
	Промежуточная аттестация	**0,1**						
	Итого	**2**		**4**				**65,9**
	Всего	**72**						

6.1. 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	1. определение информационной безопасности (ИБ), её роль в цифровой экономике; 2. триада CIA: конфиденциальность, целостность, доступность информации; 3. классификация угроз ИБ (внешние/внутренние, случайные/преднамеренные); 4. базовые модели безопасности (мандатная, дискреционная, ролевая); 5. понятие уязвимости, атаки, инцидента ИБ; 6. взаимосвязь ИБ с цифровой трансформацией бизнеса и госуправления.
2.	Нормативно-правовое регулирование ИБ в РФ и мире	1. ключевые законы РФ: 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ», 149-ФЗ «Об информации…» и др.; 2. международные стандарты (ISO/IEC 27001, GDPR); 3. требования регуляторов (ФСТЭК, ФСБ, ЦБ РФ для финсектора); 4. лицензирование и сертификация средств защиты информации; 5. ответственность за нарушения в сфере ИБ (административная, уголовная).
3.	Угрозы и риски в цифровой экономике: виды и методы противодействия.	1. типовые киберугрозы: фишинг, DDoS, APT, вредоносное ПО, социальная инженерия; 2. угрозы облачным сервисам, IoT, мобильным приложениям; 3. риски аутсорсинга ИТ-услуг и использования зарубежного ПО;

		4. методы оценки рисков (количественные и качественные); 5. стратегии управления рисками: избегание, снижение, передача, принятие.
4.	Защита персональных данных и коммерческой тайны	1. категории персональных данных, требования к их обработке; 2. технические и организационные меры защиты (шифрование, DLP-системы); 3. политика конфиденциальности и согласие на обработку данных; 4. защита коммерческой тайны: маркировка, регламенты доступа, NDA; 5. кейсы утечек данных и разбор последствий.
5.	Кибербезопасность критически важной информационной инфраструктуры (КИИ)	1. понятие КИИ, субъекты КИИ (энергетика, транспорт, финансы и т.д.); 2. требования 187-ФЗ, категорирование объектов КИИ; 3. системы обнаружения и предотвращения вторжений (IDS/IPS); 4. инцидент-менеджмент и план реагирования (IRP); 5. примеры атак на КИИ и уроки для защиты (Stuxnet, WannaCry).
6.	Криптографические методы защиты информации	1. основы криптографии: симметричное и асимметричное шифрование; 2. алгоритмы (AES, RSA, ГОСТ 34.10-2012); 3. электронная подпись и сертификаты (PKI); 4. применение в блокчейне, цифровых контрактах, платёжных системах; 5. квантовая криптография и вызовы квантовых вычислений.
7.	Безопасность облачных сервисов и распределённых систем	1. модели облачных услуг (SaaS, PaaS, IaaS) и зоны ответственности; 2. риски виртуализации и мультитенантности; 3. шифрование данных в облаке (на стороне клиента/провайдера); 4. стандарты безопасности облачных провайдеров (SOC 2, CSA); 5. гибридные и мультиоблачные архитектуры: особенности защиты.
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR	1. SIEM-системы: сбор и корреляция событий ИБ; 2. SOAR: автоматизация реагирования на инциденты; 3. EDR-решения: мониторинг конечных точек; 4. Threat Intelligence: базы индикаторов компрометации; 5. внедрение центров мониторинга ИБ (SOB)
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия	1. ИИ в кибербезопасности: анализ аномалий, прогнозирование атак; 2. блокчейн для защиты данных: неизменяемость, смарт-контракты; 3. биометрическая аутентификация: методы, точность, риски подделки;

		4. Zero Trust Architecture: принцип «не доверяй, проверяй»; 5. вызовы метавселенных и Web 3.0 для ИБ

6.2.2. Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	*Содержание практического занятия*
1.	Основы информационной безопасности	триада CIA: конфиденциальность, целостность, доступность информации; классификация угроз ИБ (внешние/внутренние, случайные/преднамеренные);
2.	Нормативно-правовое регулирование ИБ в РФ и мире	ключевые законы РФ: 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ», 149-ФЗ «Об информации…» и др.; требования регуляторов (ФСТЭК, ФСБ, ЦБ РФ для финсектора); лицензирование и сертификация средств защиты информации;
3.	Угрозы и риски в цифровой экономике: виды и методы противодействия.	методы оценки рисков (количественные и качественные);
4.	Защита персональных данных и коммерческой тайны	категории персональных данных, требования к их обработке; политика конфиденциальности и согласие на обработку данных; защита коммерческой тайны: маркировка, регламенты доступа, NDA
5.	Кибербезопасность критически важной информационной инфраструктуры (КИИ)	системы обнаружения и предотвращения вторжений (IDS/IPS); примеры атак на КИИ и уроки для защиты (Stuxnet, WannaCry).
6.	Криптографические методы защиты информации	алгоритмы (AES, RSA, ГОСТ 34.10-2012); электронная подпись и сертификаты (PKI)
7.	Безопасность облачных сервисов и распределённых систем	шифрование данных в облаке (на стороне клиента/провайдера); стандарты безопасности облачных провайдеров (SOC 2, CSA)
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR	SIEM-системы: сбор и корреляция событий ИБ; EDR-решения: мониторинг конечных точек
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия	ИИ в кибербезопасности: анализ аномалий, прогнозирование атак

6.2.3. Содержание самостоятельной работы

№	Наименование темы	*Содержание самостоятельной работы*

п/п	(раздела) дисциплины	
1.	Основы информационной безопасности	определение информационной безопасности (ИБ), её роль в цифровой экономике; триада CIA: конфиденциальность, целостность, доступность информации; классификация угроз ИБ (внешние/внутренние, случайные/преднамеренные); базовые модели безопасности (мандатная, дискреционная, ролевая); понятие уязвимости, атаки, инцидента ИБ; взаимосвязь ИБ с цифровой трансформацией бизнеса и госуправления.
2.	Нормативно-правовое регулирование ИБ в РФ и мире	ключевые законы РФ: 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ», 149-ФЗ «Об информации…» и др.; международные стандарты (ISO/IEC 27001, GDPR); требования регуляторов (ФСТЭК, ФСБ, ЦБ РФ для финсектора); лицензирование и сертификация средств защиты информации; ответственность за нарушения в сфере ИБ (административная, уголовная).
3.	Угрозы и риски в цифровой экономике: виды и методы противодействия.	типовые киберугрозы: фишинг, DDoS, APT, вредоносное ПО, социальная инженерия; угрозы облачным сервисам, IoT, мобильным приложениям; риски аутсорсинга ИТ-услуг и использования зарубежного ПО; методы оценки рисков (количественные и качественные); стратегии управления рисками: избегание, снижение, передача, принятие.
4.	Защита персональных данных и коммерческой тайны	категории персональных данных, требования к их обработке; технические и организационные меры защиты (шифрование, DLP-системы); политика конфиденциальности и согласие на обработку данных; защита коммерческой тайны: маркировка, регламенты доступа, NDA; кейсы утечек данных и разбор последствий.
5.	Кибербезопасность критически важной информационной инфраструктуры (КИИ)	понятие КИИ, субъекты КИИ (энергетика, транспорт, финансы и т.д.); требования 187-ФЗ, категорирование объектов КИИ; системы обнаружения и предотвращения вторжений (IDS/IPS); инцидент-менеджмент и план реагирования (IRP); примеры атак на КИИ и уроки для защиты (Stuxnet, WannaCry).
6.	Криптографические методы защиты	основы криптографии: симметричное и асимметричное шифрование;

	информации	алгоритмы (AES, RSA, ГОСТ 34.10-2012); электронная подпись и сертификаты (PKI); применение в блокчейне, цифровых контрактах, платёжных системах; квантовая криптография и вызовы квантовых вычислений.
7.	Безопасность облачных сервисов и распределённых систем	модели облачных услуг (SaaS, PaaS, IaaS) и зоны ответственности; риски виртуализации и мультитенантности; шифрование данных в облаке (на стороне клиента/провайдера); стандарты безопасности облачных провайдеров (SOC 2, CSA); гибридные и мультиоблачные архитектуры: особенности защиты.
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR	SIEM-системы: сбор и корреляция событий ИБ; SOAR: автоматизация реагирования на инциденты; EDR-решения: мониторинг конечных точек; Threat Intelligence: базы индикаторов компрометации; внедрение центров мониторинга ИБ (SOB)
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия	ИИ в кибербезопасности: анализ аномалий, прогнозирование атак; блокчейн для защиты данных: неизменяемость, смарт-контракты; биометрическая аутентификация: методы, точность, риски подделки; Zero Trust Architecture: принцип «не доверяй, проверяй»; вызовы метавселенных и Web 3.0 для ИБ

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

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

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Основы информационной безопасности	Опрос, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
2.	Нормативно-правовое регулирование ИБ в РФ и мире	Опрос, проблемно-аналитическое задание, исследовательский проект, творческий проект, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
3.	Угрозы и риски в цифровой экономике: виды и методы	Опрос, исследовательский проект, проблемно-аналитическое задание, тестирование.

	противодействия.	Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
4.	Защита персональных данных и коммерческой тайны	Опрос, проблемно-аналитическое задание, творческий проект. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
5.	Кибербезопасность критически важной информационной инфраструктуры (КИИ)	Опрос, проблемно-аналитическое задание, эссе. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
6.	Криптографические методы защиты информации	Опрос, исследовательский проект, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
7.	Безопасность облачных сервисов и распределённых систем	Опрос, проблемно-аналитическое задание, творческий проект. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
8.	Технологии защиты от кибератак: SIEM, SOAR, EDR	Опрос, проблемно-аналитическое задание, творческий проект. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
9.	Перспективные технологии ИБ: ИИ, блокчейн, биометрия	Опрос, проблемно-аналитическое задание, эссе. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи

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

8.2. Основная учебная литература:

1. 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

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html

8.2. Дополнительная учебная литература:

1. Информационная безопасность и правовые основы защиты персональных данных : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 с. — ISBN 978-5-8265-2648-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/141049.html

2. Автоматизация бизнес-систем: BPMS, CRM, ERP : учебное пособие / А. А. Тарасьев, Г. А. Агарков, В. М. Лаптев [и др.] ; под редакцией В. М. Лаптева. — Екатеринбург : Издательство Уральского университета, 2024. — 152 с. — ISBN 978-5-7996-3885-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/157009.html

3. Головицына, М. В. Информационные технологии в экономике : учебное пособие / М. В. Головицына. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 589 с. — ISBN 978-5-4497-2401-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133942.html

8.3. Периодические издания:

1. «Теория вероятностей и ее применения» ISSN 2305-3151
2. «Математические заметки» ISSN 2305-2880
3. «Реклама: теория и практика» ISSN2410-9622
4. «Российский журнал менеджмента» ISSN 1729-7427
5. «Экономика и математические методы» ISSN 0424-7388

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. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов». http://school-collection.edu.ru/
3. Информационные технологии моделирования и управленияhttp://www.iprbookshop.ru/43350.html
4. Философские проблемы информационных технологий и киберпространстваhttp://www.iprbookshop.ru/43489.html
5. Научный вестник Воронежского государственного архитектурно-строительного университета. Серия Информационные технологии в строительных, социальных и экономических системахhttp://www.iprbookshop.ru/64279.html

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.

При реализации программы с применением ДОТ:

Все виды занятий проводятся в форме онлайн-вебинаров с использованием современных компьютерных технологий (наличие презентации и форума для обсуждения).

В процессе изучения дисциплины студенты выполняют практические задания и промежуточные тесты. Консультирование по изучаемым темам проводится в онлайнрежиме во время проведения вебинаров и на форуме для консультаций.

Самостоятельная работа студентов складывается из следующих составляющих:

1. работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
2. внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
3. выполнение самостоятельных практических работ;

4. подготовка к экзаменам (зачетам) непосредственно перед ними.

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

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

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

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

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

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

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

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

1. Операционные системы семейства Windows;
2. Microsoft Office;
3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом;
4. Информационно-справочная система: Система КонсультантПлюс (КонсультантПлюс): веб версия;
5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (Система ГАРАНТ): веб версия;
6. Электронная информационно-образовательная система ММУ: https://elearn.mmu.ru/

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

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

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

Специализированная мебель:

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

Технические средства обучения:

Компьютер в сборе для преподавателя, проектор, экран, колонки

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Операционные системы семейства Windows, антивирус Kaspersky Endpoint Security.

КонсультантПлюс веб версия, Гарант веб версия

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк, VLC Media Player

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:

Операционные системы семейства Windows, Microsoft Office, антивирусKaspersky Endpoint Security.

КонсультантПлюс веб версия, Гарант веб версия

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк, Notepad++, Pinta, GIMP, Inkscape, OpenShot, FreeCAD, LibreCAD, Jamovi, AnyLogic, Visual Studio, Unity

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.

При реализации программы с применением ДОТ:

Все виды занятий проводятся в форме онлайн-вебинаров с использованием современных компьютерных технологий (наличие презентации и форума для обсуждения).

В процессе изучения дисциплины студенты выполняют практические задания и промежуточные тесты. Консультирование по изучаемым темам проводится в онлайнрежиме во время проведения вебинаров и на форуме для консультаций.

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

Информационная безопасность

Направление подготовки	Экономика
Код	38.03.01
Направленность (профиль)	Экономика предприятий и организаций
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные компетенции	-	ПК-19

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-19	Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	ПК-19.1 Применяет в профессиональной деятельности современные методики анализа и оценки рисков ПК-19.3 Владеет конкретными способами предупреждения рисков и управления рисками в организации

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-19**		
	– содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей;	– применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий.	– основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером; – основными понятиями и методами информационной безопасности

3.2. Критерии оценки результатов обучения по дисциплине

Шкала оценивания	Индикаторы достижения	Показатели оценивания результатов обучения
ОТЛИЧНО \ЗАЧНЕНО	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.
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».

При ответе на вопросы в рамках прохождения промежуточной аттестации (зачет/ зачет с оценкой/экзамен) допускается вольная формулировка ответа, по смыслу раскрывающая содержание ответа, указанного в фонде оценочных средств, в качестве верного ответа.

4. Типовые контрольные задания и/или иные материалы для проведения промежуточной аттестации, необходимые для оценки достижения компетенции, соотнесенной с результатами обучения по дисциплине

5 СЕМЕСТР
ПК-19

1. Что означает аббревиатура ИБ в контексте цифровой экономики?
а) Интеллектуальный бизнес.
б) Информационная безопасность.

в) Интегрированная база.
г) Инновационный бюджет.
Ответ: б) Информационная безопасность.

2. Какой из перечисленных элементов НЕ входит в триаду информационной безопасности (CIA)?
а) Конфиденциальность.
б) Целостность.
в) Актуальность.
г) Доступность.
Ответ: в) Актуальность.

3. Что такое фишинг?
а) Вид вредоносного ПО.
б) Метод шифрования данных.
в) Мошенническая попытка получить личные данные через поддельные сообщения.
г) Технология защиты сети.
Ответ: в) Мошенническая попытка получить личные данные через поддельные сообщения.

4. Какой закон РФ регулирует защиту персональных данных?
а) 135-ФЗ.
б) 152-ФЗ.
в) 44-ФЗ.
г) 273-ФЗ.
Ответ: б) 152-ФЗ.

5. Что такое DDoS-атака?
а) Атака на базу данных.
б) Распределённая атака на отказ в обслуживании.
в) Метод шифрования.
г) Вид антивирусной программы.
Ответ: б) Распределённая атака на отказ в обслуживании.

6. Какой инструмент используется для обнаружения и предотвращения вторжений?
а) IDS/IPS.
б) CRM.
в) ERP.
г) CMS.
Ответ: а) IDS/IPS.

7. Что такое ЭЦП?
а) Электронный цифровой процессор.
б) Электронно-цифровая подпись.
в) Элемент цифровой передачи.
г) Экономический цифровой показатель.
Ответ: б) Электронно-цифровая подпись.

8. Какой метод защиты данных предполагает использование ключей?
а) Шифрование.
б) Резервное копирование.
в) Аутентификация.

г) Мониторинг.
Ответ: а) Шифрование.

9. Что такое уязвимость в системе ИБ?
а) Слабое место, которое может быть использовано злоумышленником.
б) Тип антивирусной программы.
в) Способ шифрования данных.
г) Метод аутентификации.
Ответ: а) Слабое место, которое может быть использовано злоумышленником.

10. Какой стандарт регулирует системы управления информационной безопасностью?
а) ISO 9001.
б) ISO/IEC 27001.
в) ГОСТ Р 57580.
г) PCI DSS.
Ответ: б) ISO/IEC 27001.

11. Что такое двухфакторная аутентификация?
а) Использование двух паролей.
б) Использование пароля и дополнительного подтверждения (SMS, токен и т.д.).
в) Двойное шифрование данных.
г) Доступ с двух устройств.
Ответ: б) Использование пароля и дополнительного подтверждения (SMS, токен и т. д.).

12. Какой тип атаки использует поддельные веб-сайты для кражи данных?
а) Фишинг.
б) DDoS.
в) Спуфинг.
г) Вирус.
Ответ: а) Фишинг.

13. Что означает термин «киберугроза»?
а) Угроза физической безопасности.
б) Угроза, связанная с использованием информационных технологий.
в) Угроза экологической катастрофы.
г) Угроза экономического кризиса.
Ответ: б) Угроза, связанная с использованием информационных технологий.

14. Какой инструмент помогает отслеживать и анализировать события безопасности?
а) SIEM.
б) CRM.
в) ERP.
г) VPN.
Ответ: а) SIEM.

15. Что такое резервное копирование данных?
а) Удаление старых данных.
б) Создание копий данных для восстановления в случае потери.
в) Шифрование данных.
г) Передача данных по сети.
Ответ: б) Создание копий данных для восстановления в случае потери.

2. Задание на соответствие. Установите соответствие между вопросами и ответами:

	Вопрос		Ответ
1	152-ФЗ	А	Безопасность критической информационной инфраструктуры (КИИ)
2	187-ФЗ	Б	Общие вопросы информации, информационных технологий и защиты информации
3	149-ФЗ	В	Защита персональных данных граждан
4	ISO/IEC 27001	Г	Международный стандарт систем управления информационной безопасностью

Заполните соответствующие буквы под цифрами:

1	2	3	4

Ответ: 1В, 2А, 3Б, 4Г.

	Вопрос		Ответ
1	SIEM	А	Система предотвращения утечек данных, отслеживающая несанкционированную передачу информации
2	DLP	Б	Система обнаружения и предотвращения вторжений в сеть
3	IDS/IPS	В	Платформа для сбора, анализа и корреляции событий безопасности в реальном времени
4	VPN	Г	Технология создания защищённого канала для передачи данных через открытую сеть

Заполните соответствующие буквы под цифрами:

1	2	3	4

Ответ: 1В, 2А, 3Б, 4Г