Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность в цифровой экономике

Направление подготовки	Экономика
Код	38.03.01
Направленность (профиль)	Финансы в цифровой экономике
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные		ПК-19
Профессиональные		ПК-20

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
ПК-20	Способен осуществлять мониторинг, анализ и оценку социально-экономических процессов и конъюнктуры рынка финансов, банковских услуг и рынка ценных бумаг в условиях цифровой экономики	ПК-20.1 Способен проводить исследования финансовой системы, оценивать и сохранять результаты исследований, в том числе с использованием современных цифровых технологий. ПК-20.5 Способен применять цифровые инструменты и технологии при осуществлении контроля финансово-экономической деятельности

3. Описание планируемых результатов обучения по

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		
	принципы работы юриста с источниками информации, знать методы ее сбора, селекции, проверки и анализа. - принципы работы современной	- применять принципы работы юриста с источниками информации. - использовать современную техническую базу и новейшие цифровые	-навыками работы с электронными базами данных. - навыками работы с информацией в глобальных компьютерных сетях. - навыками выполнения

	технической базы и новейшие цифровые технологии, применяемые для решения профессиональных задач. - основные должностные обязанности по обеспечению законности и правопорядка, безопасности личности, общества, государства при использовании современных технических баз и информации	технологии, применяемые для решения профессиональных задач. - использовать современную техническую базу и новейшие цифровые технологии, применяемые для решения профессиональных задач	должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства при использовании современных технических баз и информации.
Код компетенции	**ПК-20**		
	- методику проведения исследований финансовой системы, оценки и сохранения результатов исследований, в том числе с использованием современных цифровых технологий.	- применять цифровые инструменты и технологии при осуществлении контроля финансово-экономической деятельности	- цифровыми инструментами и технологиями при осуществлении контроля финансово-экономической деятельности

4.Место дисциплины (модуля) в структуре образовательной программы

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

Данная дисциплина взаимосвязана с другими дисциплинами, такими как «Финансы», «Планирование и прогнозирование в экономике», «Финансовые вычисления», «Бухгалтерский финансовый учет и отчетность», «Финансовое планирование и бюджетирование».

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

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: Финансы в цифровой экономике.

5.Объем дисциплины

Виды учебной работы	***Формы обучения***

	Очная	***Очно-заочная***	***Очно-заочная с применением ДОТ***
Общая трудоемкость: зачетные единицы/часы	2/72	2/72	2/72
Контактная работа:			
Занятия лекционного типа	18	16	2
Занятия семинарского типа	18	16	4
Промежуточная аттестация: **зачет**	0,1	0,1	0,1
Самостоятельная работа (СРС)	35,9	39,9	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

6.1.2. 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 раб.*	*Иные занятия*	
1.	Введение в безопасность информации современного предприятия Основные понятия, термины и определения в области защиты информации	3		3				6
2.	Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности	3		3				6
3.	Законодательная и нормативная база правового регулирования	4		4				10

	вопросов защиты информации Доктрина информационной безопасности Российской Федерации.							
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	4		4				6
5.	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	4		4				7,9
	Всего	**18**		**18**				**35,9**
	Промежуточная аттестация	**0,1**						

6.1.2. Очно-заочная 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.	Введение в безопасность информации современного предприятия Основные понятия, термины и определения в области защиты информации	3		3				8
2.	Актуальность проблемы защиты	3		3				8

	информации. Виды угроз и рисков информационной безопасности							
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.	4		4				8
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	3		3				8
5.	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	3		3				7,9
	Всего	**16**		**16**				**39,9**
	Промежуточная аттестация	**0,1**						

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 раб.*	*Иные занятия*	
1.	Введение в безопасность информации современного предприятия Основные понятия, термины и	1						13

	определения в области защиты информации							
2.	Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности	1						13
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.			2				13
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.			1				13
5.	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии			1				13,9
	Промежуточная аттестация	**0,1**						
	Итого	**2**		**4**				**65,9**

-

6.2. Программа дисциплины, структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1.	Введение в безопасность информации современного предприятия Основные понятия, термины и определения в области защиты информации	Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации

2.	Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности	Виды угроз и рисков информационной безопасности Формирование модели угроз: угрозы, реализуемые через технические каналы утечки информации, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах или вспомогательных технических средствах и системах; угрозы реализуемые за счет несанкционированного доступа к персональным данным. Модель угроз и модель нарушителя информационной безопасности. Риски информационной безопасности.
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.	Доктрина информационной безопасности Российской Федерации. Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы президента Российской Федерации. Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Порядок проведения инвентаризации персональных данных.
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	Подготовка к аттестации на соответствие положениям ФЗ №152 Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации, информационных технологий и непрерывности бизнеса. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства РФ. Ответственность за правонарушения в области защиты информации
5	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	Комплексная система обеспечения информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности организации Типовая структура, задачи и функции подразделения (службы) информационной безопасности организации. Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

6.2.2. Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Введение в безопасность информации современного предприятия Основные понятия, термины и определения в области защиты	Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации

	информации	
2.	Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности	Виды угроз и рисков информационной безопасности Формирование модели угроз: угрозы, реализуемые через технические каналы утечки информации, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах или вспомогательных технических средствах и системах; угрозы реализуемые за счет несанкционированного доступа к персональным данным. Модель угроз и модель нарушителя информационной безопасности. Риски информационной безопасности.
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.	Доктрина информационной безопасности Российской Федерации. Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы президента Российской Федерации. Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Порядок проведения инвентаризации персональных данных.
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	Подготовка к аттестации на соответствие положениям ФЗ №152 Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации, информационных технологий и непрерывности бизнеса. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства РФ. Ответственность за правонарушения в области защиты информации
5.	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	Комплексная система обеспечения информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности организации Типовая структура, задачи и функции подразделения (службы) информационной безопасности организации. Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

6.2.3. Содержание самостоятельной работы

№ п/п	**Наименование темы (раздела) дисциплины**	**Содержание самостоятельной работы**
1.	Введение в безопасность информации современного предприятия Основные понятия, термины и определения в области защиты информации	Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации
	Актуальность проблемы	Виды угроз и рисков информационной

2.	защиты информации. Виды угроз и рисков информационной безопасности	безопасности Формирование модели угроз: угрозы, реализуемые через технические каналы утечки информации, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах или вспомогательных технических средствах и системах; угрозы реализуемые за счет несанкционированного доступа к персональным данным. Модель угроз и модель нарушителя информационной безопасности. Риски информационной безопасности.
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.	Доктрина информационной безопасности Российской Федерации. Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы президента Российской Федерации. Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Порядок проведения инвентаризации персональных данных.
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	Подготовка к аттестации на соответствие положениям ФЗ №152 Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации, информационных технологий и непрерывности бизнеса. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства РФ. Ответственность за правонарушения в области защиты информации
5	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	Комплексная система обеспечения информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности организации Типовая структура, задачи и функции подразделения (службы) информационной безопасности организации. Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

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.	Введение в безопасность информации современного предприятия Основные понятия,	Опрос, информационный проект Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.

	термины и определения в области защиты информации	
2.	Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности	Опрос, проблемно-аналитическое задание, эссе. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
3.	Законодательная и нормативная база правового регулирования вопросов защиты информации Доктрина информационной безопасности Российской Федерации.	Исследовательский проект, письменный опрос. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
4.	Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	Опрос, диспут-игра. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
5	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	Опрос, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.

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

8.1 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

8.2 Дополнительная учебная литература:

1. Информационные системы и технологии. Часть 1: монография / В. Д. Колдаев, И. В. Гелета, Ю. А. Бобель, Р. М. Сафина. — Москва: Перо, Центр научной мысли, 2011. — 126 с. — ISBN 978-5-91940-150-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/8982.html

2. Лучанинов, Д. В. Основы разработки web-сайтов образовательного назначения:

учебное пособие / Д. В. Лучанинов. — Саратов: Ай Пи Эр Медиа, 2018. — 105 с. — ISBN 978-5-4486-0174-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/70775.html

2. Дементьева, Ю. В. Основы работы с электронными образовательными ресурсами: учебное пособие / Ю. В. Дементьева. — Саратов: Вузовское образование, 2017. — 80 с. — ISBN 978-5-906172-21-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/62066.html

8.3. Периодические издания

1. Вестник Волгоградского государственного университета. Серия 5. Юриспруденция http://www.iprbookshop.ru/7276.html
2. Вопросы современной юриспруденции http://www.iprbookshop.ru/48791.html

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

1. Федеральный портал «Российское образование» https://dic.academic.ru/
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
3. Информационно-коммуникационные технологии в образовании: федеральный образовательный портал http://ict.edu.ru/
4. Интернет-университет информационных технологий (ИНТУИТ.ру) http://www.intuit.ru/
5. Информатика и ИКТ в образовании http://www.rusedu.info
6. Тесты по информатике и информационным технологиям http://www.junior.ru/wwwexam/
7. Федеральный центр информационных образовательных ресурсов http://fcior.edu.ru/catalog/osnovnoe_obshee/

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.

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.

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.

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, разрабатываются адаптированные для инвалидов программы подготовки с учетом различных нозологий, виды и формы сопровождения обучения, используются специальные технические и программные средства обучения, дистанционные образовательные технологии, обеспечивается безбарьерная среда и прочее.

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 в цифровой экономике

Направление подготовки	Экономика
Код	38.03.01
Направленность (профиль)	Финансы в цифровой экономике
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные		ПК-19
Профессиональные		ПК-20

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
ПК-20	Способен осуществлять мониторинг, анализ и оценку социально-экономических процессов и конъюнктуры рынка финансов, банковских услуг и рынка ценных бумаг в условиях цифровой экономики	ПК-20.1 Способен проводить исследования финансовой системы, оценивать и сохранять результаты исследований, в том числе с использованием современных цифровых технологий. ПК-20.5 Способен применять цифровые инструменты и технологии при осуществлении контроля финансово-экономической деятельности

3. Описание планируемых результатов обучения по

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**		
	принципы работы юриста с источниками информации, знать методы ее сбора, селекции, проверки и анализа. - принципы работы современной	- применять принципы работы юриста с источниками информации. - использовать современную техническую базу и новейшие цифровые технологии,	-навыками работы с электронными базами данных. - навыками работы с информацией в глобальных компьютерных сетях. - навыками

	технической базы и новейшие цифровые технологии, применяемые для решения профессиональных задач. - основные должностные обязанности по обеспечению законности и правопорядка, безопасности личности, общества, государства при использовании современных технических баз и информации	применяемые для решения профессиональных задач. - использовать современную техническую базу и новейшие цифровые технологии, применяемые для решения профессиональных задач	выполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства при использовании современных технических баз и информации.
Код компетенции	**ПК-20**		
	- методику проведения исследований финансовой системы, оценки и сохранения результатов исследований, в том числе с использованием современных цифровых технологий.	- применять цифровые инструменты и технологии при осуществлении контроля финансово-экономической деятельности	- цифровыми инструментами и технологиями при осуществлении контроля финансово-экономической деятельности

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.
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, соотнесенной с результатами обучения по дисциплине**

СЕМЕСТР 5
ПК-19

1. Перечислите виды информационной безопасности:

А)Персональная, корпоративная, государственная

Б) Локальная, глобальная, смешенная;

В) Клиентская, серверная, техническая;

2. Дайте определение понятию «Кибербезопасность»…

А) совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры;

Б) область информационных технологий, направленная на получение доступа к персональным, корпоративным и государственным данным;

В)совокупность методов и практик защиты от несанкционированного доступа злоумышленников к компьютерам, серверам, мобильным устройствам, электронным системам, сетям и к данным;

3. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации является:

А) Источником информации;

Б) Носителем информации;

В) Обладателем информации;

4. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:

А) Электронная база данных;

Б) Информационные технологии;

В) **Информационно-телекоммуникационная сеть;**

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:

А) Доступ к информации;

Б) Шифрование информации;

В) Конфиденциальность информации;

6.Что такое персональные данные?

А) это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Б) это определенная информация, не относящаяся к прямо определенному, или определяемому физическому лицу, а также юридическому лицу (субъекту персональных данных) ;

В) частичная информация, относящаяся к прямо определенному, или определяемому физическому лицу и юридическому лицу (субъекту и объекту персональных данных);

7. Что относится к специальным категориям персональных данных?

А) физиологические особенности человека, а также информация о дате и месте рождения;
Б) национальная принадлежность, политические взгляды, религиозные или философские убеждения;
В) личные сведения (паспортные данные, номер телефона, сведения об образовании и профессии;

8. Что такое информационная безопасность?
А) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
Б) практика предотвращения санкционированного доступа, для использования, раскрытия, искажения, изменения, исследования для передачи информации третьим лицам;
В) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб информационной безопасности;

9. Отношения, связанные с обработкой персональных данных, регулируются законом…
А) Приказом Президента «Об информации, информационных технологиях»;
Б) Федеральным законом «О защите информации»;
В) Федеральным законом «О персональных данных»;

10. Действия с персональными данными (согласно федеральному закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т.д это:
А) «Исправление персональных данных»;
Б) «Работа с персональными данными»;
В) **«Обработка персональных данных»;**

11. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных

ему) действий в системах с ограниченным доступом называется:

А) Авторизация;

Б) Аутентификация;

В) **Идентификация.**

12. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

А) Идентификация;

Б) Аутентификация;

В) **Шифрование.**

13. В Федеральном законе «О персональных данных» выделяют следующие категории персональных данных:

А) главные, дополнительные, специальные;

Б) личные, публичные, государственные;

В) общедоступные, специальные, биометрические.

14.Что такое «деобезличивание» персональных данных?

А) действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными;

Б) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному объекту персональных данных возможно определить без дополнительной информации;

В) действия, в результате которых становится невозможным без использования специальной информации определить принадлежность персональных данных конкретному лицу, обладателю персональных данных.

15. Что понимается под «обезличенные персональные данные»?

А) это данные, находящиеся в электронных системах, принадлежность которых конкретному объекту персональных данных возможно определить без дополнительной информации;

Б) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно

определить без дополнительной информации;

В) это персональные данные, хранимые в электронных информационных базах, которые принадлежат определенным субъектам персональных данных.

16. Дайте определение понятию «Государственная тайна»…

А) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности;

Б) режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

В) совокупность информационных ресурсов, позволяющие при существующих обстоятельствах с помощью специальных информационных систем безопасности не допустить несанкционированный доступ к сведениям.

17. Что такое «коммерческая тайна»?

А) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности.

Б) совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

В) режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

18. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен законодательством РФ:

А). Дисциплинарные взыскания;

Б) Административный ответственность;

В) Смертная казнь.

19. Информационная безопасность обеспечивает…

А) Блокирование информации;

Б) Искажение информации;

В) Сохранность информации;

20. Что такое киберпреступления?

А) преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства;

Б) преступная деятельность, целью которой является передача, сбор, похищение или хранение в целях передачи сведений, составляющих государственную тайну;

В) преступная деятельность, целью которой является правомерное использование компьютера, компьютерной сети или сетевого устройства;

СЕМЕСТР 5
ПК-20

1. Что такое «фишинг»?

А) тип кибератаки, которую злоумышленники используют для взлома системы или сети;

Б) вид интернет-мошенничества, цель которого получить идентификационные данные пользователей;

В) тип кибератаки с помощью заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО;

2. Для защиты от злоумышленников необходимо использовать:

А) Системное программное обеспечение;

Б) Прикладное программное обеспечение;

В) Антивирусные программы;

3. Что такое «ЭЦП»?

А) электронно-цифровой процессор;

Б) электронная цифровая подпись;

В) электронно-цифровой преобразователь.

4. Информация, составляющая государственную тайну не может иметь гриф…

А) «для служебного пользования»;

Б) «секретно»;

В) «совершенно секретно»;

5. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

А) атака;

Б) угроза;

В) уязвимость.

6. Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных?

А) субъект персональных данных;

Б)оператор информационной системы;

В) **оператор персональных данных.**

7. Дайте определение «Оператор персональных данных» по ФЗ «О персональных данных»….

А) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и/или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Б) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

В) это данные, хранимые в информационных системах в электронном виде,

принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

8. Какой подход к обеспечению безопасности имеет место?

А) логический;

Б) математический;

В) комплексный.

9. Основными объектами информационной безопасности являются:

А) Компьютерные сети, базы данных;

Б) Информационные системы, государственные системы;

В) Бизнес-ориентированные, коммерческие системы.

10. Федеральный закон «О персональных данных»

А) ФЗ № 153 от 27.06.2006;

Б) ФЗ № 152 от 27.07.2006;

В) ФЗ № 150 от 27.08.2006.

11.Под информационной безопасностью понимается…

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

12.Защита информации – это..

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

13.От чего зависит информационная безопасность?

А) **от компьютеров**

Б) от поддерживающей инфраструктуры

В) от информации

14.Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

15.Доступность – это…

А) **возможность за приемлемое время получить требуемую информационную услугу.**

Б) логическая независимость

В) нет правильного ответа

16.Целостность – это..

А) **целостность информации**

Б) непротиворечивость информации

В) защищенность от разрушения

17.Конфиденциальность – это..

А) **защита от несанкционированного доступа к информации**

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

18.Для чего создаются информационные системы?

А) **получения определенных информационных услуг**

Б) обработки информации

В) все ответы правильные

19.Целостность можно подразделить:

А) **статическую**

Б) динамичную

В) структурную

20.Где применяются средства контроля динамической целостности?

А) **анализе потока финансовых сообщений**

Б) обработке данных

В) **при выявлении кражи, дублирования отдельных сообщений**