

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность

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

Москва
2025

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

Группа компетенций	Категория компетенций	Код
Общепрофессиональные		ОПК-3
Профессиональные		ПК-2

2. Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-3	Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.1 Знает понятие, виды и особенности продуктов и услуг в сфере ИКТ; основы алгоритмизации, современные методологии разработки программных средств; этапы разработки программных средств; методы обеспечения информационной безопасности. ОПК-3.2 Умеет разрабатывать алгоритмы и программы для практической реализации продуктов и услуг в сфере ИКТ. ОПК-3.3 Владеет методами управления процессами создания и использования продуктов и услуг в сфере ИКТ, в частности, навыками разработки алгоритмов и программ для их практической реализации.
ПК-2	Умеет проектировать, создавать и внедрять компоненты ИТ-инфраструктуры предприятия, обеспечивающие достижение стратегических целей предприятия и поддержку бизнес-процессов	ПК-2.1. Знает основы электротехники и электроники, особенности вычислительных систем, теорию сетей и телекоммуникаций, особенности функционирования корпоративных информационных систем, основы управления интеллектуальной собственностью ПК-2.2. Умеет разрабатывать бизнес-планы, проводить публичные презентации, применять знания в области информационных технологий для проектирования компонентов ИТ-инфраструктуры предприятий ПК-2.3. Владеет навыками постановки задач и заказа на технологические

		исследования ИТ для бизнеса, их координирования и последующего анализа, определения статей расходов и доходов, разработки ценовой политики и стратегии развития ИТ-инфраструктуры предприятия, подбора персонала для создания и внедрения компонентов ИТ-инфраструктуры, заказа патентной экспертизы технологических разработок организации, анализа бизнес-эффективности существующих у организации активов и формированию предложений по приобретению при необходимости сторонних активов
--	--	---

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	ОПК-3		
	роль и задачи информационной безопасности на предприятии; - техническое и программное обеспечение для решения задач информационной безопасности (ИБ); - методы и средства защиты информации; - вероятные угрозы ИБ.	- формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; - использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в профессиональной деятельности.	навыками реализации мер по обеспечению ИБ с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий и вероятных угроз; - инструментальными средствами защиты информации; - навыками обеспечения целостности, доступности и конфиденциальности информации; - навыками работы по реализации политики информационной безопасности.
Код компетенции	ПК-2		
	Принципы	Разрабатывать	Навыками работы с

проектирования ИТ-инфраструктуры, включая сетевые архитектуры, системы хранения данных и облачные решения, соответствующие стратегии предприятия.	технические задания и архитектурные решения для компонентов ИТ-инфраструктуры с учетом требований безопасности и масштабируемости.	инструментами проектирования (например, Microsoft Visio, Enterprise Architect) и управления конфигурациями (Ansible, Terraform).
Современные технологии и стандарты (ITIL, COBIT, TOGAF) для управления ИТ-услугами и интеграции бизнес-процессов.	Координировать взаимодействие между подразделениями (бизнес-аналитики, разработчики, эксплуатация) для успешного внедрения ИТ-систем.	Опытном внедрения ERP-, CRM-систем или корпоративных сервисов (1C, SAP, Microsoft Dynamics) в соответствии с бизнес-требованиями.
Методы оценки эффективности внедряемых ИТ-решений и их влияния на ключевые показатели бизнеса (KPI).	Анализировать риски и предлагать оптимизацию ИТ-инфраструктуры для снижения затрат и повышения надежности.	Методами мониторинга и аудита ИТ-инфраструктуры для обеспечения ее соответствия стратегическим целям компании.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к факультативной части учебного плана ОПОП.

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

Изучение дисциплины позволит обучающимся реализовывать универсальные и общекультурные компетенции в профессиональной деятельности.

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

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: бизнес-информатика.

5. Объем дисциплины

<i>Виды учебной работы</i>	<i>Формы обучения</i>	
	<i>очная форма</i>	<i>Очно-заочная форма</i>
Общая трудоемкость: зачетные единицы/часы	4/144	4/144
Контактная работа:		

Занятия лекционного типа	40	22
Занятия семинарского типа	40	22
Промежуточная аттестация: зачет с оценкой	0,1	0,15
Самостоятельная работа (СРС)	63,9	99,85

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)			
		Аудиторная работа			Самостоятел ьная работа
		ЛЗ	ПЗ	ЛабЗ	
1	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	7	7	-	10
2	Нормативно - законодательная база и стандарты в области информационной безопасности	7	7	-	10
3	Угрозы информационной безопасности, их классификация и анализ.	7	7	-	10
4	Методы и средства обеспечения информационной безопасности.	7	7	-	10
5	Информационная безопасность автоматизированных систем	7	7	-	10
6	Информационная безопасность компьютеров и компьютерных сетей	5	5	-	13,9
	Промежуточная аттестация	0,1			
	Итого	40	40	-	63,9

6.1.1. Очно-заочная форма обучения

№ п/п	Раздел/тема	Виды учебной работы (в часах)			
		Аудиторная работа			Самостоятел ьная работа
		ЛЗ	ПЗ	ЛабЗ	
1	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	2	2	-	17
2	Нормативно - законодательная база и стандарты в области информационной безопасности	2	2	-	17
3	Угрозы информационной безопасности, их классификация и анализ.	4	4	-	17
4	Методы и средства обеспечения информационной безопасности.	4	4	-	17
5	Информационная безопасность автоматизированных систем	4	4	-	17

6	Информационная безопасность компьютеров и компьютерных сетей	4	4	-	15,85
	Промежуточная аттестация	0,15			
	Итого	22	22	-	99,85

6.2. Программа дисциплины структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного курса
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	Цели и задачи курса, общая характеристика его содержания. Основные понятия и определения. Понятие национальной и информационной безопасности РФ. Основные составляющие информационной безопасности. Национальные интересы, безопасность и основные угрозы безопасности России в информационной сфере. Государственная информационная политика. Государственная тайна. Место информационной безопасности экономических систем в национальной безопасности страны.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности	Основные нормативно-справочные документы. Законодательная база информационной безопасности. Доктрина информационной безопасности РФ. Отечественные и зарубежные стандарты в области информационной безопасности. Руководящие документы Федеральной службы по техническому и экспортному контролю.
3.	Угрозы информационной безопасности, их классификация и анализ.	Понятие угрозы. Виды угроз. Нарушители информационной безопасности. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз. Классификация угроз по способам их негативного воздействия и на основе методов системного анализа. Классификация атак, уровни безопасности.
4.	Методы и средства обеспечения информационной безопасности.	Организационно-административные, технические, криптографические методы защиты информации. Модели каналов передачи информации. Коды, обнаруживающие и исправляющие ошибки. Защита информации в автоматизированных системах обработки данных. Аппаратная и программная реализация симметричных и асимметричных криптографических систем. Защита системы и данных в современных ОС. Механизмы информационной безопасности. Идентификация и аутентификация, управление доступом.

5.	Информационная безопасность автоматизированных систем	Информационные системы и связанные с их функционированием угрозы. Причины нарушения целостности информации и возможные злоумышленные действия в автоматизированных системах обработки данных. Модель нарушителя информационных систем. Модели информационной безопасности и их использование. Таксономия и анализ способов нарушения информационной безопасности. Модели оценки угроз. Модели защиты информации. Методы определения требований к защите информации. Функции и стратегии защиты информации. Архитектура систем защиты информации.
6.	Информационная безопасность компьютеров и компьютерных сетей	Цели, функции и задачи защиты информации в компьютерах и компьютерных сетях. Информационная безопасность в условиях функционирования в России глобальных сетей. Архитектура механизмов защиты информации. Разработка защищенных приложений в средах программирования. Принципы и средства защиты электронной почты. Методы защиты межсетевых обмена данными, использование межсетевых экранов. Компьютерные вирусы и их классификация. Способы заражения программ. Методы защиты. Антивирусные программы. Программно-технические средства защиты информации в компьютере.

6.2.2. Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	Вопросы: 1. Основные составляющие информационной безопасности. 2. Интересы и угрозы в области национальной безопасности. 3. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. 4. Задачи защиты информации на современном этапе 5. Основные положения государственной информационной политики.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности	Вопросы: 1. Что такое законодательный уровень информационной безопасности? 2. В чем состоит отличительная особенность стандарта шифрования AES от DES? 3. Что собой представляет конфиденциальная информация?

		4. Что собой представляет электронная подпись? 5. Какие виды требований входят в «Общие критерии»?
3.	Угрозы информационной безопасности, их классификация и анализ.	Вопросы: 1. Назовите наиболее выраженные угрозы информационной безопасности 2. Каков характер происхождения угроз? 3. Каковы предпосылки появления угроз? 4. Назовите известные вам подходы к классификации угроз. 5. Классификация угроз по способам их негативного воздействия.
4.	Методы и средства обеспечения информационной безопасности.	Вопросы: 1. Что относится к основным аспектам информационной безопасности? 2. Что собой представляют криптографические методы и средства защиты информации? 3. Административный уровень информационной безопасности. 4. Основные классы мер процедурного уровня 5. Основные понятия программно-технического уровня информационной безопасности.
5.	Информационная безопасность автоматизированных систем	Вопросы: 1. Что такое модель безопасности? 2. Методы оценки уязвимости информации. 3. Методы создания защищенных систем обработки информации. 4. Модели политик безопасности и их сравнение. 5. Составляющие теоретических основ методов защиты информационных
6.	Информационная безопасность компьютеров и компьютерных сетей	Вопросы: 1. Задачи защиты информации в компьютерах и компьютерных сетях. 2. Что такое криптографические протоколы? 3. Каковы функции межсетевого экрана? 4. Программно-технические средства защиты информации в ПК 5. Классификация компьютерных вирусов.

6.2.3. Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Формы и тематика самостоятельной работы
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	Первоочередные мероприятия по реализации государственной политики обеспечения Изучение информационных процессов. Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами
2.	Нормативно - законодательная база и	Законодательный уровень информационной безопасности

	стандарты в области информационной безопасности	Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами
3.	Угрозы информационной безопасности, их классификация и анализ.	Классификация угроз Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
4.	Методы и средства обеспечения информационной безопасности.	Административный уровень информационной безопасности Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
5.	Информационная безопасность автоматизированных систем	Модели политик безопасности и их сравнение Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания
6.	Информационная безопасность компьютеров и компьютерных сетей	Программно-технические средства защиты информации в ПК Реферирование литературы Работа со справочными материалами Работа с Интернет-ресурсами Индивидуальные задания

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

В рамках текущего контроля преподаватель самостоятельно может проводить следующие мероприятия:

№ п/п	Контролируемые разделы (темы)	Формы текущего контроля
1.	Основные понятия информационной безопасности и ее место в системе национальной безопасности РФ.	Вопросы к занятию, тестирование.
2.	Нормативно - законодательная база и стандарты в области информационной безопасности	Вопросы к занятию, интерактивные занятия, тестирование.
3.	Угрозы информационной безопасности, их классификация и анализ.	Вопросы к занятию, практические задания, тестирование.
4.	Методы и средства обеспечения информационной безопасности.	Вопросы к занятию, практические задания, тестирование.
5.	Информационная безопасность автоматизированных систем	Вопросы к занятию, практические задания, информационные проекты, тестирование.
6.	Информационная безопасность компьютеров и компьютерных сетей	Вопросы к занятию, информационные проекты, тестирование.

8. Перечень основной и дополнительной учебной литературы, необходимой для

освоения дисциплины (модуля)

1.1.Основная учебная литература:

1. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/77320.html>

2. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : Евразийский открытый институт, 2010. — 328 с. — ISBN 978-5-374-00381-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/10746.html>

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

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

1.2.Дополнительная учебная литература:

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

2. Алешин А.П. Техническое обеспечение безопасности бизнеса (2-е издание) [Электронный ресурс]/ Алешин А.П.— Электрон. текстовые данные.— М.: Дашков и К, Ай Пи Эр Медиа, 2017. — 160 с.— Режим доступа: <http://www.iprbookshop.ru/57143>

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

8.3. Периодические издания

1. Журнал «Компьютерра» <http://www.computerra.ru>

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

1. Федеральный портал «Российское образование». <http://www.edu.ru/>

2. Электронно-библиотечная система IPR BOOKS <https://www.iprbookshop.ru/>

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

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекционных занятий, практических занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев полноценного высшего образования, на которую отводится значительная часть учебного времени.

Самостоятельная работа студентов складывается из следующих составляющих:

- работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
- внеаудиторная подготовка к контрольным работам, выполнение докладов,

рефератов и курсовых работ;

- выполнение самостоятельных практических работ;
- подготовка к экзаменам (зачетам) непосредственно перед ними.

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

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

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

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

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

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

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

1. Microsoft Windows Server;
2. Семейство ОС Microsoft Windows;
3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом;
4. Информационно-справочная система: Система КонсультантПлюс (КонсультантПлюс);
5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (Система ГАРАНТ);

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

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

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

Специализированная мебель:

Комплект учебной мебели (стол, стул) по количеству обучающихся; комплект мебели для

преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя, проектор, экран, колонки.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows 10, КонсультантПлюс, Система ГАРАНТ, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype, Zoom.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду ММУ.

12.2. Помещение для самостоятельной работы обучающихся.

Специализированная мебель:

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

Технические средства обучения:

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

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

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

Перечень свободно распространяемого программного обеспечения:

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

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ММУ.

13. Образовательные технологии, используемые при освоении дисциплины

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

На учебных занятиях используются технические средства обучения – проектор, ноутбук, проекционный экран, колонки для демонстрации слайдов, видеосюжетов и др. Тестирование обучаемых может осуществляться с использованием компьютерного оборудования университета.

13.1. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:

- чтение проблемно-информационных лекций с использованием доски и видеоматериалов;
- 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.

**Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ДИСЦИПЛИНЕ**

Информационная безопасность

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

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

Группа компетенций	Категория компетенций	Код
Общепрофессиональные		ОПК-3
Профессиональные		ПК-2

4. Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-3	Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.1 Знает понятие, виды и особенности продуктов и услуг в сфере ИКТ; основы алгоритмизации, современные методологии разработки программных средств; этапы разработки программных средств; методы обеспечения информационной безопасности. ОПК-3.2 Умеет разрабатывать алгоритмы и программы для практической реализации продуктов и услуг в сфере ИКТ. ОПК-3.3 Владеет методами управления процессами создания и использования продуктов и услуг в сфере ИКТ, в частности, навыками разработки алгоритмов и программ для их практической реализации.
ПК-2	Умеет проектировать, создавать и внедрять компоненты ИТ-инфраструктуры предприятия, обеспечивающие достижение стратегических целей предприятия и поддержку бизнес-процессов	ПК-2.1. Знает основы электротехники и электроники, особенности вычислительных систем, теорию сетей и телекоммуникаций, особенности функционирования корпоративных информационных систем, основы управления интеллектуальной собственностью ПК-2.2. Умеет разрабатывать бизнес-планы, проводить публичные презентации, применять знания в области информационных технологий для проектирования компонентов ИТ-инфраструктуры предприятий ПК-2.3. Владеет навыками постановки задач и заказа на технологические исследования ИТ для бизнеса, их

		координирования и последующего анализа, определения статей расходов и доходов, разработки ценовой политики и стратегии развития ИТ-инфраструктуры предприятия, подбора персонала для создания и внедрения компонентов ИТ-инфраструктуры, заказа патентной экспертизы технологических разработок организации, анализа бизнес-эффективности существующих у организации активов и формированию предложений по приобретению при необходимости сторонних активов
--	--	---

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	ОПК-3		
	роль и задачи информационной безопасности на предприятии; - техническое и программное обеспечение для решения задач информационной безопасности (ИБ); - методы и средства защиты информации; - вероятные угрозы ИБ.	- формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; - использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в профессиональной деятельности.	навыками реализации мер по обеспечению ИБ с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий и вероятных угроз; - инструментальными средствами защиты информации; - навыками обеспечения целостности, доступности и конфиденциальности информации; - навыками работы по реализации политики информационной безопасности.
Код компетенции	ПК-2		
	Принципы проектирования	Разрабатывать технические задания и	Навыками работы с инструментами

	ИТ-инфраструктуры, включая сетевые архитектуры, системы хранения данных и облачные решения, соответствующие стратегии предприятия. Современные технологии и стандарты (ITIL, COBIT, TOGAF) для управления ИТ-услугами и интеграции бизнес-процессов. Методы оценки эффективности внедряемых ИТ-решений и их влияния на ключевые показатели бизнеса (KPI).	архитектурные решения для компонентов ИТ-инфраструктуры с учетом требований безопасности и масштабируемости. Координировать взаимодействие между подразделениями (бизнес-аналитики, разработчики, эксплуатация) для успешного внедрения ИТ-систем. Анализировать риски и предлагать оптимизацию ИТ-инфраструктуры для снижения затрат и повышения надежности.	проектирования (например, Microsoft Visio, Enterprise Architect) и управления конфигурациями (Ansible, Terraform). Опытом внедрения ERP-, CRM-систем или корпоративных сервисов (1C, SAP, Microsoft Dynamics) в соответствии с бизнес-требованиями. Методами мониторинга и аудита ИТ-инфраструктуры для обеспечения ее соответствия стратегическим целям компании.
--	--	--	---

3.2. Критерии оценки результатов обучения по дисциплине

Шкала оценивания	Индикаторы достижения	Показатели оценивания результатов обучения
ОТЛИЧНО/ЗАЧТЕНО	Знает:	- студент глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- студент умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.
	Владеет:	- студент владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; - При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями

		руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО/ЗАЧТЕНО	Знает:	- студент твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- студент умеет самостоятельно и в основном правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя научные понятия и ссылки на нормативную базу.
	Владеет:	- студент в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
УДОВЛЕТВОРИТЕЛЬНО/ЗАЧТЕНО	Знает:	- студент ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- студент в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- студент владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
Компетенция не достигнута		

НЕУДОВЛЕТВОРИТЕЛЬН О/НЕЗАЧТЕНО	Знает:	- студент не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.
	Умеет:	студент не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым “удовлетворительно”.

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 (закрытого, открытого и иного типа) для проведения промежуточной аттестации, необходимые для оценки достижения компетенции, соотнесенной с результатами обучения по дисциплине.

6 СЕМЕСТР ОПК-3

1.Какие существуют основные уровни обеспечения защиты информации?

- А) законодательный
- Б) административный
- В) программно-технический
- Г) вероятностный
- Д) процедурный

✓ Правильные ответы: А, Б, В, Д

Ответ: А, Б, В, Д

2.С чем связана основная причина потерь информации в компьютерных сетях?

- А) с глобальным хищением информации
- Б) с появлением интернета
- В) с недостаточной образованностью в области безопасности ✓
- Г) с плохими законами
- Д) с техническими сбоями

Ответ: В

3.К аспектам ИБ относятся:

- А) дискретность
- Б) целостность ✓
- В) конфиденциальность ✓
- Г) актуальность
- Д) доступность ✓

Ответ: Б, В, Д

4. Что такое несанкционированный доступ?

- А) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа ✓
- Б) Создание резервных копий в организации
- В) Правила для обхода парольной защиты
- Г) Вход в систему без согласования с руководителем организации
- Д) Удаление не нужной информации

Ответ: А

5. Что такое целостность информации?

- А) возможность ее изменения любым субъектом
- Б) возможность изменения только единственным пользователем
- В) существование в виде единого набора файлов
- Г) существование в неискаженном виде ✓
- Д) автоматическое резервное копирование

Ответ: Г

6. Что такое аутентификация?

- А) Проверка количества переданной и принятой информации
- Б) Проверка подлинности идентификации ✓
- В) Проверка подлинности информации
- Г) Определение файлов, из которых удалена служебная информация
- Д) Проверка скорости передачи данных

Ответ: Б

7. Утечка информации

- А) несанкционированное изменение информации
- Б) ознакомление постороннего лица с содержанием секретной информации ✓
- В) потеря данных
- Г) уменьшение объема информации
- Д) автоматическое архивирование

Ответ: Б

8. Основные программы для защиты от компьютерных вирусов

- А) Программы-сканеры ✓
- Б) Программы-мониторы ✓
- В) Программы-детекторы ✓
- Г) Программы-фильтры ✓
- Д) Программы-рекорды

Ответ: А, Б, В, Г

9. Отметьте функции, которые должны осуществлять средства защиты:

- А) Разграничение доступа к вычислительным ресурсам и информации ✓
- Б) Несанкционированный доступ к системе
- В) Идентификация субъектов и объектов ✓
- Г) Разграничение вычислительных ресурсов и информации
- Д) Регистрация действий в системе ✓

Ответ: А, В, Д

10. Сервисы безопасности:

- А) идентификация и аутентификация ✓
 - Б) шифрование ✓
 - В) инверсия паролей
 - Г) контроль целостности ✓
 - Д) регулирование конфликтов
- Ответ: А, Б, Г

11.Классификация компьютерных вирусов

- А) по деструктивным возможностям ✓
 - Б) по размеру
 - В) по среде обитания ✓
 - Г) по особенностям алгоритма ✓
 - Д) по способу заражения ✓
- Ответ: А, В, Г, Д

12.К методам защиты от НСД относятся

- А) уменьшение доступа
 - Б) разграничение доступа ✓
 - В) увеличение доступа
 - Г) приостановка доступа
 - Д) аутентификация и идентификация ✓
- Ответ: Б, Д

13.Совокупность правил, процедур, принципов в области ИБ, которыми руководствуется организация в своей деятельности называется

- А) политикой информации
 - Б) защитой информации
 - В) политикой безопасности ✓
 - Г) организацией безопасности
 - Д) системой защиты
- Ответ: В

14.Как подразделяются вирусы в зависимости от деструктивных возможностей?

- А) Сетевые, файловые, загрузочные
 - Б) Безвредные, неопасные, опасные ✓
 - В) Резидентные, нерезидентные
 - Г) Полиморфные, макровирусы, вирусы-невидимки, "паразитические"
 - Д) Шифрованные, стелс-вирусы
- Ответ: Б

15.Причины возникновения ошибок в данных

- А) Погрешность измерений ✓
 - Б) Неверная интерпретация данных ✓
 - В) Ошибки при переносе данных с промежуточного документа в компьютер ✓
 - Г) Использование недопустимых методов анализа данных ✓
 - Д) Преднамеренное искажение данных ✓
- Ответ: А, Б, В, Г, Д

16.Наиболее эффективное средство для защиты от сетевых атак

- А) использование сетевых экранов ✓

- Б) использование антивирусных программ
 - В) посещение только «надёжных» Интернет-источников
 - Г) использование только сертифицированных программ
 - Д) регулярное обновление ПО
- Ответ: А

17.Простейший способ идентификации в КС:

- А) Токен
- Б) Password
- В) Пароль ✓
- Г) Login
- Д) Смарт-карта

Ответ: В

18.Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами:

- А) Антивирус
- Б) Замок
- В) Брандмауэр ✓
- Г) Криптография
- Д) Экспертная система

Ответ: В

19.Хищение информации – это...

- А) Несанкционированное копирование информации ✓
- Б) Утрата информации
- В) Блокирование информации
- Г) Искажение информации
- Д) Продажа информации

Ответ: А

20.Троянские программы бывают:

- А) утилиты удалённого администрирования ✓
- Б) программы - шпионы ✓
- В) рекламные программы ✓
- Г) программы удаления данных на локальном компьютере ✓
- Д) программы резервного копирования

Ответ: А, Б, В, Г

21.Сетевые черви бывают:

- А) Web-черви ✓
- Б) почтовые черви ✓
- В) черви операционной системы
- Г) черви MS Office
- Д) черви баз данных

Ответ: А, Б

22.К биометрическим системам защиты информации относятся системы идентификации по:

- А) отпечаткам пальцев ✓
- Б) радужной оболочке глаза ✓

- В) росту
 - Г) весу
 - Д) цвету глаз
 - Е) характеристикам речи ✓
- Ответ: А, Б, Е

23. Достоинства симметричных ключей

- А) Высокая скорость шифрования ✓
- Б) Низкая скорость шифрования
- В) Меньшая длина ключей ✓
- Г) Большая длина ключей
- Д) Простота реализации ✓

Ответ: А, В, Д

24. Формой правовой защиты литературных, художественных и научных произведений является (...) право

- А) литературное
- Б) художественное
- В) авторское ✓
- Г) патентное
- Д) интеллектуальное

Ответ: В

25. Какой документ определяет стратегические направления обеспечения информационной безопасности в РФ?

- А) Федеральный закон "О персональных данных"
- Б) Доктрина информационной безопасности РФ ✓
- В) ГОСТ Р 57580.1-2017
- Г) Указ Президента "О национальных целях развития"

Ответ: Б

ПК-2

1. К какому виду безопасности относится информационная безопасность в системе национальной безопасности РФ?

- А) Экономическая
- Б) Видовой компонент национальной безопасности ✓
- В) Социальная
- Г) Экологическая

Ответ: Б

2. Что включает в себя понятие "информационная безопасность государства"?

- А) Только защиту персональных данных
- Б) Защиту информационных ресурсов, инфраструктуры и суверенитета в информационном пространстве ✓
- В) Безопасность компьютерных сетей предприятий
- Г) Контроль за интернет-трафиком

Ответ: Б

3. Какой закон регулирует защиту персональных данных в РФ?

- А) ФЗ-152 "О персональных данных" ✓

- Б) ФЗ-149 "Об информации, информационных технологиях и о защите информации"
 - В) ФЗ-187 "О безопасности критической информационной инфраструктуры"
 - Г) ФЗ-161 "О национальной платежной системе"
- Ответ: А

4.Какой стандарт информационной безопасности применяется для организаций банковской сферы?

- А) ПДн (СТБ ГОСТ Р 57580) ✓
 - Б) ISO 9001
 - В) ГОСТ Р 7.0.97-2016
 - Г) PCI DSS
- Ответ: А

5.Какой документ определяет требования к защите информации в государственных информационных системах?

- А) Приказ ФСТЭК №17 ✓
 - Б) ГОСТ Р ИСО/МЭК 27001
 - В) ФЗ-135 "О защите конкуренции"
 - Г) Указ Президента №400
- Ответ: А

6.К какому типу угроз относится фишинг?

- А) Социальная инженерия ✓
 - Б) Аппаратные сбои
 - В) Природные катастрофы
 - Г) Ошибки программного обеспечения
- Ответ: А

7.Что такое АРТ-атака?

- А) Целенаправленная многоэтапная кибератака ✓
 - Б) Вирус-шифровальщик
 - В) Спам-рассылка
 - Г) DDoS-атака
- Ответ: А

8.Какой угрозе соответствует несанкционированный доступ к информации?

- А) Нарушение конфиденциальности ✓
 - Б) Нарушение целостности
 - В) Нарушение доступности
 - Г) Физическое уничтожение данных
- Ответ: А

9.Что является основой системы разграничения доступа?

- А) Политика RBAC (Role-Based Access Control) ✓
 - Б) Антивирусное ПО
 - В) Резервное копирование
 - Г) Межсетевые экраны
- Ответ: А

10.Какой метод защиты обеспечивает невозможность отказа от авторства?

- А) Электронная цифровая подпись (ЭП) ✓

- Б) Шифрование
 - В) Аутентификация
 - Г) Хеширование
- Ответ: А

11. Какой стандарт описывает лучшие практики управления информационной безопасностью?

- А) ISO/IEC 27001 ✓
 - Б) ITIL
 - В) COBIT
 - Г) TOGAF
- Ответ: А

12. Что такое "аудит информационной безопасности"?

- А) Систематическая проверка соответствия ИБ-политикам ✓
 - Б) Установка антивирусов
 - В) Настройка VPN
 - Г) Обучение сотрудников
- Ответ: А

13. Какой компонент АС обеспечивает защиту от НСД?

- А) Подсистема разграничения доступа ✓
 - Б) Система мониторинга
 - В) Резервный сервер
 - Г) База данных
- Ответ: А

14. Что относится к средствам криптографической защиты информации (СКЗИ)?

- А) Сертифицированные ФСБ РФ алгоритмы шифрования ✓
 - Б) Антивирус Касперского
 - В) Межсетевой экран
 - Г) SIEM-система
- Ответ: А

15. Какой протокол обеспечивает безопасную передачу данных в интернете?

- А) TLS/SSL ✓
 - Б) HTTP
 - В) FTP
 - Г) SMTP
- Ответ: А

16. Что такое IDS в контексте сетевой безопасности?

- А) Система обнаружения вторжений (Intrusion Detection System) ✓
 - Б) Система управления идентификацией
 - В) Средство резервного копирования
 - Г) Инструмент мониторинга трафика
- Ответ: А

17. Какой тип атаки направлен на переполнение буфера памяти?

- А) Buffer Overflow ✓
- Б) Phishing

В) Spoofing
Г) Sniffing
Ответ: А

18. Для защиты от чего предназначен VPN?
А) От перехвата данных в публичных сетях ✓
Б) От вирусов
В) От DDoS
Г) От спама
Ответ: А

19. Какой принцип защиты реализует технология "песочницы" (sandbox)?
А) Изоляция потенциально опасных процессов ✓
Б) Шифрование данных
В) Аутентификация пользователей
Г) Фильтрация трафика
Ответ: А

20. Какой орган в РФ отвечает за сертификацию средств защиты информации?
А) ФСТЭК России ✓
Б) Минцифры
В) Роскомнадзор
Г) Центробанк
Ответ: А

21. Что такое "инцидент информационной безопасности"?
А) Событие, приводящее к нарушению конфиденциальности/целостности/доступности данных ✓
Б) Установка обновлений ПО
В) Плановый аудит
Г) Обучение сотрудников
Ответ: А

22. Какой метод защиты эффективен против ransomware?
А) Регулярное резервное копирование ✓
Б) Использование сложных паролей
В) Настройка брандмауэра
Г) Фильтрация email
Ответ: А

23. Что проверяет система SIEM?
А) События безопасности в режиме реального времени ✓
Б) Скорость интернета
В) Исправность жестких дисков
Г) Температуру процессора
Ответ: А

24. Какой закон регулирует использование криптографии в РФ?
А) ФЗ-63 "Об электронной подписи" ✓
Б) ФЗ-152
В) ФЗ-149

Г) ФЗ-187

Ответ: А

25. Что означает принцип "минимальных привилегий" в ИБ?

А) Предоставление пользователям только необходимых прав ✓

Б) Запрет на резервное копирование

В) Использование простых паролей

Г) Отказ от антивирусов

Ответ: А