Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность и защита данных

Направление подготовки	Информационные системы и технологии
Код	09.03.02
Направленность (профиль)	Информационные технологии и большие данные
Квалификация (степень) выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-4

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-4	**ПК-4.** Способен применять методы и средства проектирования программного обеспечения и баз данных	**ПК-4.1.** Адаптация бизнес-процессов к возможностям типовой ИС. Разработка модели бизнес-процессов. Проектирование и дизайн типовой ИС. Моделирование бизнес-процессов **ПК-4.2.** Сбор данных о запросах и потребностях заказчика применительно к типовой ИС. Документирование собранных данных в соответствии с регламентами организации. **ПК-4.3.** Согласование и утверждение требований к типовой ИС. **ПК-4.4.** Разработка прототипов ИС на базе типовой ИС в соответствии с требованиями. **ПК-4.5.** Интеграция ИС с существующими ИС заказчика **ПК-4.6.** Модульное и интеграционное тестирование ИС. **ПК-4.7.** Создание руководства администратора, руководства программиста и пользовательской документации к модифицированным элементам типовой ИС **ПК-4.8.** Знание отраслевой нормативной технической документации **ПК-4.9.** Проведение приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. **ПК-4.10.** Документальное оформление результата приемо-сдаточных испытаний в соответствии с установленными регламентами. **ПК-4.11.** Согласование документации.

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-4**		
	- методы оценки объемов и сроков выполнения работ, технологии выполнения работ в организации; - архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы; - основы современных операционных систем, основы современных систем управления базами данных, устройство и функционирование современных ИС; теорию баз данных, системы хранения и анализа баз данных; - основы программирования, современные объектно-ориентированные языки программирования, современные структурные языки программирования, языки современных бизнес-приложений; - современные методики тестирования разрабатываемых ИС, современные стандарты информационного взаимодействия	- работать с современными системами программирования, конструировать программное обеспечение и базы данных, разрабатывать основные программные документы; - оценивать объемы и сроки выполнения работ; - разрабатывать руководство программиста к модифицированным элементам типовой ИС; - разрабатывать руководство администратора к модифицированным элементам типовой ИС; - разрабатывать руководство пользователя к модифицированным элементам типовой ИС; - разрабатывать ТЗ.	- навыками конструирования программного обеспечения и баз данных; - навыками разработки интерфейсов обмена данными, форматов обмена данными, технологий обмена данными между ИС и существующими системами в соответствии с техническим заданием.

	систем; - программные средства и платформы инфраструктуры информационных технологий организаций; - современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM); - основы теории систем и системного анализа; - методики описания и моделирования бизнес-процессов, средства моделирования бизнес-процессов; - системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников; - отраслевую нормативную техническую документацию.		

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность и защита данных» относится к части, формируемой участниками образовательных отношений учебного плана ОПОП. Данная дисциплина взаимосвязана с другими дисциплинами, такими как: «Алгоритмизация и методы программирования», «Операционные системы и среды», «Компьютерные сети», «Управление рисками», «Теория систем и системный анализ», «Базы данных». В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов:

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: Информационные технологии и большие данные

5. Объем дисциплины

Виды учебной работы	*Формы обучения*
	Очно-заочная
Общая трудоемкость: зачетные единицы/часы	4/144
Контактная работа:	
Занятия лекционного типа	24
Занятия семинарского типа	12
Промежуточная аттестация: **зачет**	0,1
Самостоятельная работа (СРС)	107,9

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

6.1. Распределение часов по разделам/темам и видам работы

6.1.1. 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.	Основы информационной безопасности	3			1			15
2.	Средства защиты от вредоносного ПО и доверенной загрузки	3			1			15
3.	Межсетевые экраны и системы предотвращения вторжений	3			2			15
4.	Мониторинг и анализ защищённости	3			2			15
5.	Изолированные среды и виртуализация	3			2			15
6.	Криптографическая защита и резервное копирование	3			2			15
7.	Защита операционных систем и систем ИИ	3			2			17,9
	Промежуточная аттестация	**0,1**						
	Итого	**24**			**12**			**107,9**

6.2 Программа дисциплины, структурированная по темам / разделам

6.2.1 Содержание лекционного курса

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1.	Основы информационной безопасности	Понятие информационной безопасности, её цели и задачи. Основные угрозы информационной безопасности. Принципы обеспечения информационной безопасности: конфиденциальность, целостность, доступность. Нормативно-правовая база в области информационной безопасности (ФЗ № 149, ФЗ № 152, ФЗ № 187 и др.).
2.	Средства защиты от вредоносного ПО и доверенной загрузки	Классификация вредоносного программного обеспечения. Средства антивирусной защиты: принципы работы, виды, примеры решений (Kaspersky, Dr.Web, ESET и т.д.). Средства доверенной загрузки: назначение, механизмы контроля целостности, примеры реализаций (например, «Аккорд-АМДЗ», «Соболь»).
3.	Межсетевые экраны и системы предотвращения вторжений	Межсетевой экран (Firewall): функции, типы (пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы), примеры (Cisco ASA, iptables, pfSense). Межсетевой экран уровня веб-приложений (WAF): назначение, сценарии применения, примеры (ModSecurity, Cloudflare WAF). Система предотвращения вторжений (IPS): принципы работы, интеграция с другими средствами защиты, примеры (Snort, Suricata).
4.	Мониторинг и анализ защищённости	Система мониторинга информационной безопасности (SIEM): назначение, архитектура, функции (сбор и корреляция событий, отчётность). Средства анализа защищённости: сканеры уязвимостей (Nessus, OpenVAS), пентест-инструменты (Metasploit). Методы выявления и реагирования на инциденты ИБ.
5.	Изолированные среды и виртуализация	Изолированная среда исполнения программ (песочница): назначение, технологии реализации (Sandboxie, Cuckoo Sandbox). СЗИ виртуализации и контейнеризации: особенности защиты виртуальных машин и контейнеров (Docker, Kubernetes), гипервизоры с поддержкой безопасности. Однонаправленный шлюз: принцип работы, области применения (критическая инфраструктура, АСУ ТП).
6.	Криптографическая защита и резервное копирование	Основы криптографии: симметричные и асимметричные алгоритмы (AES, RSA), хэш-функции. Средства криптографической защиты информации: СКЗИ (ViPNet, КриптоПро

		CSP), протоколы защищённой передачи данных (TLS, IPsec). Средства резервного копирования: стратегии (полный, инкрементальный, дифференциальный бэкап), решения (Veeam, Acronis, Backup Exec).
7.	Защита операционных систем и систем ИИ	Защищённые операционные системы: требования к ОС с повышенными мерами безопасности (SELinux, Astra Linux). Защита систем искусственного интеллекта: угрозы (отравление данных, состязательные атаки), методы защиты моделей и данных. Средства защиты информации от несанкционированного доступа (СЗИ НСД): аутентификация, авторизация, контроль доступа (Active Directory, LDAP).

6.2.2 Содержание практических занятий

№ п/п	Наименование раздела дисциплины	Содержание практических занятий
1.	Основы информационной безопасности	Понятие информационной безопасности, её цели и задачи. Основные угрозы информационной безопасности. Принципы обеспечения информационной безопасности: конфиденциальность, целостность, доступность. Нормативно-правовая база в области информационной безопасности (ФЗ № 149, ФЗ № 152, ФЗ № 187 и др.).
2.	Средства защиты от вредоносного ПО и доверенной загрузки	Классификация вредоносного программного обеспечения. Средства антивирусной защиты: принципы работы, виды, примеры решений (Kaspersky, Dr.Web, ESET и т.д.). Средства доверенной загрузки: назначение, механизмы контроля целостности, примеры реализаций (например, «Аккорд-АМДЗ», «Соболь»).
3.	Межсетевые экраны и системы предотвращения вторжений	Межсетевой экран (Firewall): функции, типы (пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы), примеры (Cisco ASA, iptables, pfSense). Межсетевой экран уровня веб-приложений (WAF): назначение, сценарии применения, примеры (ModSecurity, Cloudflare WAF). Система предотвращения вторжений (IPS): принципы работы, интеграция с другими средствами защиты, примеры (Snort, Suricata).
4.	Мониторинг и анализ защищённости	Система мониторинга информационной безопасности (SIEM): назначение, архитектура, функции (сбор и корреляция событий, отчётность). Средства анализа защищённости: сканеры уязвимостей (Nessus, OpenVAS), пентест-инструменты (Metasploit). Методы выявления и реагирования на инциденты ИБ.

5.	Изолированные среды и виртуализация	Изолированная среда исполнения программ (песочница): назначение, технологии реализации (Sandboxie, Cuckoo Sandbox). СЗИ виртуализации и контейнеризации: особенности защиты виртуальных машин и контейнеров (Docker, Kubernetes), гипервизоры с поддержкой безопасности. Однонаправленный шлюз: принцип работы, области применения (критическая инфраструктура, АСУ ТП).
6.	Криптографическая защита и резервное копирование	Основы криптографии: симметричные и асимметричные алгоритмы (AES, RSA), хэш-функции. Средства криптографической защиты информации: СКЗИ (ViPNet, КриптоПро CSP), протоколы защищённой передачи данных (TLS, IPsec). Средства резервного копирования: стратегии (полный, инкрементальный, дифференциальный бэкап), решения (Veeam, Acronis, Backup Exec).
7.	Защита операционных систем и систем ИИ	Защищённые операционные системы: требования к ОС с повышенными мерами безопасности (SELinux, Astra Linux). Защита систем искусственного интеллекта: угрозы (отравление данных, состязательные атаки), методы защиты моделей и данных. Средства защиты информации от несанкционированного доступа (СЗИ НСД): аутентификация, авторизация, контроль доступа (Active Directory, LDAP).

6.2.3 Содержание самостоятельной работы

№ п/п	**Наименование раздела дисциплины**	**Содержание самостоятельной работы**
1.	Основы информационной безопасности	Понятие информационной безопасности, её цели и задачи. Основные угрозы информационной безопасности. Принципы обеспечения информационной безопасности: конфиденциальность, целостность, доступность. Нормативно-правовая база в области информационной безопасности (ФЗ № 149, ФЗ № 152, ФЗ № 187 и др.).
2.	Средства защиты от вредоносного ПО и доверенной загрузки	Классификация вредоносного программного обеспечения. Средства антивирусной защиты: принципы работы, виды, примеры решений (Kaspersky, Dr.Web, ESET и т.д.). Средства доверенной загрузки: назначение, механизмы контроля целостности, примеры реализаций (например, «Аккорд-АМДЗ», «Соболь»).
3.	Межсетевые экраны и системы предотвращения	Межсетевой экран (Firewall): функции, типы (пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы), примеры (Cisco ASA, iptables, pfSense). Межсетевой экран уровня

	вторжений	веб-приложений (WAF): назначение, сценарии применения, примеры (ModSecurity, Cloudflare WAF). Система предотвращения вторжений (IPS): принципы работы, интеграция с другими средствами защиты, примеры (Snort, Suricata).
4.	Мониторинг и анализ защищённости	Система мониторинга информационной безопасности (SIEM): назначение, архитектура, функции (сбор и корреляция событий, отчётность). Средства анализа защищённости: сканеры уязвимостей (Nessus, OpenVAS), пентест-инструменты (Metasploit). Методы выявления и реагирования на инциденты ИБ.
5.	Изолированные среды и виртуализация	Изолированная среда исполнения программ (песочница): назначение, технологии реализации (Sandboxie, Cuckoo Sandbox). СЗИ виртуализации и контейнеризации: особенности защиты виртуальных машин и контейнеров (Docker, Kubernetes), гипервизоры с поддержкой безопасности. Однонаправленный шлюз: принцип работы, области применения (критическая инфраструктура, АСУ ТП).
6.	Криптографическая защита и резервное копирование	Основы криптографии: симметричные и асимметричные алгоритмы (AES, RSA), хэш-функции. Средства криптографической защиты информации: СКЗИ (ViPNet, КриптоПро CSP), протоколы защищённой передачи данных (TLS, IPsec). Средства резервного копирования: стратегии (полный, инкрементальный, дифференциальный бэкап), решения (Veeam, Acronis, Backup Exec).
7.	Защита операционных систем и систем ИИ	Защищённые операционные системы: требования к ОС с повышенными мерами безопасности (SELinux, Astra Linux). Защита систем искусственного интеллекта: угрозы (отравление данных, состязательные атаки), методы защиты моделей и данных. Средства защиты информации от несанкционированного доступа (СЗИ НСД): аутентификация, авторизация, контроль доступа (Active Directory, LDAP).

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

В рамках текущего контроля преподаватель самостоятельно может проводить следующие мероприятия:

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Основы информационной безопасности	Опрос, проблемно-аналитическое задание.

2.	Средства защиты от вредоносного ПО и доверенной загрузки	Опрос, проблемно-аналитическое задание, тестирование.
3.	Межсетевые экраны и системы предотвращения вторжений	Опрос, проблемно-аналитическое задание.
4.	Мониторинг и анализ защищённости	Опрос, проблемно-аналитическое задание, тестирование.
5.	Изолированные среды и виртуализация	Опрос, проблемно-аналитическое задание.
6.	Криптографическая защита и резервное копирование	Опрос, проблемно-аналитическое задание, тестирование.
7.	Защита операционных систем и систем ИИ	Опрос, проблемно-аналитическое задание, тестирование.

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

8.1. Основная литература:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html
2. Информационная безопасность и правовые основы защиты персональных данных : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 с. — ISBN 978-5-8265-2648-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/141049.html
3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html

8.2. Дополнительная литература:

1. Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/143637.html
2. Информационная безопасность : учебное пособие / И. Б. Тесленко, Д. В. Виноградов, А. М. Губернаторов [и др.] ; под редакцией И. Б. Тесленко. — Владимир : Издательство Владимирского государственного университета, 2023. — 212 с. — ISBN 978-5-9984-1783-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/143816.html

8.3. Периодические издания

1. Вестник Московского государственного технического университета имени Н.Э. Баумана. Серия Естественные науки. ISSN 1812-3368.

https://www.iprbookshop.ru/23124.html
2. Открытые Системы. СУБД. ISSN 1028-7493. https://www.iprbookshop.ru/76383.html
3. Информационные технологии моделирования и управления. ISSN 1813-9744. https://www.iprbookshop.ru/43350.html

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

1. Федеральный портал «Российское образование» http://www.edu.ru
2. Электронно-библиотечная система «Научная электронная библиотека eLIBRARY.RU» https://www.elibrary.ru
3. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru
4. Электронная библиотечная система https://biblioclub.ru

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

5. Федеральный портал «Российское образование» http://www.edu.ru
6. Электронно-библиотечная система «Научная электронная библиотека eLIBRARY.RU» https://www.elibrary.ru
7. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru
8. Электронная библиотечная система https://biblioclub.ru

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:

1. Работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
2. Внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
3. Выполнение самостоятельных практических работ;
4. Подготовка к экзаменам (зачетам) непосредственно перед ними.

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

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

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

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

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

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

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

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

1. 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, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк.

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, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк, 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 – лекции (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация); и семинарские (практические) занятия, так и активные и интерактивные формы занятий - деловые и ролевые игры, решение ситуационных задач и разбор конкретных ситуаций.

На учебных занятиях используются технические средства обучения мультимедийной аудитории: компьютер, монитор, колонки, настенный экран, проектор, микрофон, пакет программ Microsoft Office для демонстрации презентаций и медиафайлов, видеопроектор для демонстрации слайдов, видеосюжетов и др. Тестирование обучаемых может осуществляться с использованием компьютерного оборудования университета.

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

- чтение проблемно-информационных лекций с использованием доски и видеоматериалов;
- семинарские занятия для обсуждения, дискуссий и обмена мнениями;
- контрольные опросы;
- консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками;
- подготовка и обсуждение рефератов (проектов), презентаций (научно-исследовательская работа);
- тестирование по основным темам дисциплины.

13.2. Активные и интерактивные методы и формы обучения

Из перечня видов: («*мозговой штурм», анализ НПА, анализ проблемных ситуаций, анализ конкретных ситуаций, инциденты, имитация коллективной профессиональной деятельности, разыгрывание ролей, творческая работа, связанная с освоением дисциплины, ролевая игра, круглый стол, диспут, беседа, дискуссия, мини-конференция и др.*) используются следующие:

- *диспут;*
- *анализ проблемных, творческих заданий, ситуационных задач;*
- *ролевая игра;*
- *круглый стол;*
- *мини-конференция;*

- *дискуссия;*
- *беседа.*

13.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее – инвалиды и лица с ОВЗ) с целью обеспечения их прав. При обучении учитываются особенности их психофизического развития, индивидуальные возможности и при необходимости обеспечивается коррекция нарушений развития и социальная адаптация указанных лиц.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально-технического обеспечения, особенностями восприятия учебной информации студентов с инвалидностью 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

Объектно-ориентированное программирование

Направление подготовки	Информационные системы и технологии
Код	09.03.02
Направленность (профиль)	Информационные технологии и большие данные
Квалификация (степень) выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-4

2. **Компетенции и индикаторы их достижения**

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-4	**ПК-4.** Способен применять методы и средства проектирования программного обеспечения и баз данных	**ПК-4.1.** Адаптация бизнес-процессов к возможностям типовой ИС. Разработка модели бизнес-процессов. Проектирование и дизайн типовой ИС. Моделирование бизнес-процессов **ПК-4.2.** Сбор данных о запросах и потребностях заказчика применительно к типовой ИС. Документирование собранных данных в соответствии с регламентами организации. **ПК-4.3.** Согласование и утверждение требований к типовой ИС. **ПК-4.4.** Разработка прототипов ИС на базе типовой ИС в соответствии с требованиями. **ПК-4.5.** Интеграция ИС с существующими ИС заказчика **ПК-4.6.** Модульное и интеграционное тестирование ИС. **ПК-4.7.** Создание руководства администратора, руководства программиста и пользовательской документации к модифицированным элементам типовой ИС **ПК-4.8.** Знание отраслевой нормативной технической документации **ПК-4.9.** Проведение приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. **ПК-4.10.** Документальное оформление результата приемо-сдаточных испытаний в соответствии с установленными регламентами. **ПК-4.11.** Согласование документации.

3. **Описание планируемых результатов обучения по дисциплине**

3.1. Описание планируемых результатов обучения по дисциплине

Планируемые результаты обучения по дисциплине представлены дескрипторами

(знания, умения, навыки).

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-4**		
	- методы оценки объемов и сроков выполнения работ, технологии выполнения работ в организации; - архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы; - основы современных операционных систем, основы современных систем управления базами данных, устройство и функционирование современных ИС; теорию баз данных, системы хранения и анализа баз данных; - основы программирования, современные объектно-ориентированные языки программирования, современные структурные языки программирования, языки современных бизнес-приложений; - современные методики тестирования разрабатываемых ИС, современные стандарты информационного	- работать с современными системами программирования, конструировать программное обеспечение и базы данных, разрабатывать основные программные документы; - оценивать объемы и сроки выполнения работ; - разрабатывать руководство программиста к модифицированным элементам типовой ИС; - разрабатывать руководство администратора к модифицированным элементам типовой ИС; - разрабатывать руководство пользователя к модифицированным элементам типовой ИС; - разрабатывать ТЗ.	- навыками конструирования программного обеспечения и баз данных; - навыками разработки интерфейсов обмена данными, форматов обмена данными, технологий обмена данными между ИС и существующими системами в соответствии с техническим заданием.

	взаимодействия систем; - программные средства и платформы инфраструктуры информационных технологий организаций; - современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM); - основы теории систем и системного анализа; - методики описания и моделирования бизнес-процессов, средства моделирования бизнес-процессов; - системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников; - отраслевую нормативную техническую документацию.		

3.2. Критерии оценки знаний студентов

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”.

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

ТЕСТИРОВАНИЕ

7 СЕМЕСТР
ПК-4

1. **Что такое доверенная загрузка?**

a) Процесс загрузки операционной системы без проверки.
b) **Процесс загрузки, при котором проверяется целостность и подлинность загрузочных компонентов.**
c) Процесс, не требующий никакой проверки.

2. Какой из следующих методов используется антивирусами для обнаружения вирусов?

a) **Сигнатурный анализ.**
b) Анализ поведения без базы данных.
c) Интуитивный анализ.

3. Что такое система предотвращения вторжений (IPS)?

a) Система, которая только фиксирует инциденты.
b) **Система, которая активно блокирует подозрительную активность.**
c) Система, не требующая настройки.

4. Какова основная функция межсетевого экрана?

a) Защита от вирусов.
b) **Фильтрация трафика между сетями.**
c) Шифрование данных.

5. Какой из следующих методов мониторинга безопасности является наиболее распространенным?

a) **Системы SIEM.**
b) Ручной анализ логов.
c) Использование антивирусов.

6. Что такое изолированная среда исполнения программ?

a) Среда, где программы могут взаимодействовать без ограничений.
b) **Среда, в которой программы исполняются в изоляции от основной системы.**
c) Среда, где программы не могут быть запущены.

7. Какой из следующих методов защиты информации является криптографическим?

a) Файловые права доступа.
b) **Шифрование данных.**
c) Антивирусная защита.

8. Какова основная задача средств резервного копирования?

a) Удаление ненужных данных.
b) **Восстановление данных после их утраты.**
c) Защита от вирусов.

9. Что такое межсетевой экран уровня веб-приложений?

a) Устройство, фильтрующее только почтовый трафик.
b) **Устройство, защищающее веб-приложения от атак.**
c) Устройство, не требующее конфигурации.

10. Какой из следующих методов анализа защищенности используется для оценки уязвимостей?

a) **Пентестинг.**
b) Ручное тестирование.
c) Мониторинг трафика.

11. Что такое однонаправленный шлюз?

a) Устройство, позволяющее двустороннюю передачу данных.

b) **Устройство, позволяющее передавать данные только в одном направлении.**
c) Устройство, не требующее настройки.

12. Какой из следующих элементов является частью системы мониторинга информационной безопасности?
a) Файловая система.
b) **Система управления событиями и информацией безопасности (SIEM).**
c) Операционная система.

13. Какой из следующих методов защиты предназначен для предотвращения несанкционированного доступа?
a) **Аутентификация пользователей.**
b) Резервное копирование данных.
c) Шифрование файлов.

14. Какой из следующих аспектов важен для защиты систем искусственного интеллекта?
a) **Защита данных для обучения и предотвращение манипуляций.**
b) Увеличение вычислительных мощностей.
c) Открытый доступ к алгоритмам.

15. Какой из следующих методов используется для защиты виртуализированных сред?
a) **Средства защиты информации виртуализации/контейнеризации.**
b) Использование только антивирусов.
c) Отключение сетевых интерфейсов.

16. Какой из следующих методов резервного копирования является наиболее безопасным?
a) Резервное копирование на локальный диск.
b) **Резервное копирование в облако с шифрованием.**
c) Резервное копирование на USB-накопитель.

17. Какой из следующих подходов используется для защиты данных в облачных сервисах?
a) **Шифрование данных перед загрузкой в облако.**
b) Хранение данных в открытом виде.
c) Использование стандартных паролей.

18. Какой из следующих методов анализа защищенности используется для оценки уязвимостей?
a) **Сканирование уязвимостей.**
b) Ручное тестирование.
c) Мониторинг трафика.

19. Какой из следующих методов предотвращает атаки на веб-приложения?
a) Отключение всех внешних соединений.
b) **Использование межсетевого экрана уровня веб-приложений.**
c) Установка антивируса на сервер.

20. Что такое криптографическая защита информации?

a) Процесс, при котором информация становится доступной для всех.
b) **Процесс шифрования данных для защиты от несанкционированного доступа.**
c) Процесс создания резервных копий данных.