Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Разработка, сопровождение и обеспечение безопасности информационных систем

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

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-2

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-2	**ПК-2.** Способен использовать математический аппарат и современные компьютерные средства для выполнения научно-исследовательских работ по закрепленной тематике	**ПК-2.3.** Способен использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве. **ПК-2.4.** Собирает и анализирует информацию по решаемой задаче, составляет ее математическое описание, обеспечивает накопление, анализ и систематизацию собранных данных с использованием современных достижений науки и информационных систем; **ПК-2.5.** Выявляет и формулирует актуальные научные проблемы; обосновывать актуальность, теоретическую и практическую значимость темы научного исследования, разрабатывать план и программу проведения научного исследования;

3. Описание планируемых результатов обучения по дисциплине

3.1. <u>Описание планируемых результатов обучения по дисциплине</u>

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-2**		
	Основы операционных систем: Знать архитектуру и основные компоненты	Конфигурировать операционные системы: Уметь устанавливать и	Практическими навыками конфигурирования: Владеть навыками

	операционных систем (например, Windows, Linux). Знать принципы работы файловых систем и управления процессами. Сетевые протоколы: Знать основные сетевые протоколы (TCP/IP, HTTP, HTTPS, FTP) и их функции. Знать принципы работы сетевых устройств (маршрутизаторов, коммутаторов, брандмауэров). Инструменты конфигурирования: Знать инструменты и утилиты для конфигурирования операционных систем и сетевых устройств (например, командная строка, PowerShell, SSH). Безопасность: Знать основные принципы и методы обеспечения безопасности операционных систем и сетевых устройств.	настраивать операционные системы для веб-разработки. Уметь управлять пользователями и правами доступа в операционных системах. Настраивать сетевые устройства: Уметь конфигурировать маршрутизаторы и коммутаторы для обеспечения сетевой связности. Уметь настраивать брандмауэры для защиты веб-приложений. Использовать инструменты командной строки: Уметь использовать командную строку для выполнения задач администрирования и конфигурирования. Уметь применять скрипты для автоматизации процессов конфигурирования. Обеспечивать безопасность систем: Уметь применять методы шифрования и аутентификации для защиты данных. Уметь проводить аудит безопасности и выявлять уязвимости в системах.	установки и настройки операционных систем в средах веб-разработки. Владеть навыками конфигурирования сетевых устройств для оптимизации работы веб-приложений. Работой с документацией: Владеть умением читать и интерпретировать техническую документацию по операционным системам и сетевым устройствам. Решением проблем: Владеть навыками диагностики и устранения неполадок в операционных системах и сетевых устройствах. Работой в команде: Владеть навыками взаимодействия с другими специалистами (разработчиками, системными администраторами) для эффективного конфигурирования и поддержки веб-приложений.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Разработка, сопровождение и обеспечение безопасности информационных систем» относится к части, формируемой участниками образовательных отношений учебного плана ОПОП.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как:

«Проектирование высоконагруженных систем», «Базы данных», «Web-разработка», «Практикум по автоматизации внедрения и эксплуатации новых систем» и пр.

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: 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	12
Занятия семинарского типа	24
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 занятия*	
1	Введение в информационные системы	1		3				11
2	Методы и технологии разработки информационных систем	1		2				11
3	Безопасность информационных систем	1		3				11
4.	Управление информационными ресурсами	1		3				11
5	Современные тенденции в разработке	1		2				11

	информационных систем							
6	Управление проектами в области информационных технологий	1		2				11
7	Интеграция информационных систем	3		3				13
8	Анализ и оптимизация производительности информационных систем	3		3				18
9	Резервное копирование и восстановление данных	3		3				10,9
	Промежуточная аттестация	**0,1**						
	Итого	**12**		**24**				**107,9**

6.2. Программа дисциплины, структурированная по темам / разделам

6.2.1. Содержание лекционных занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1	Введение в информационные системы	- Обзор основных понятий и терминов - Роль информационных систем в современном мире - Основные принципы построения информационных систем
2	Методы и технологии разработки информационных систем	- Программные платформы для разработки ИС - Методологии разработки информационных систем - Принципы построения пользовательского интерфейса
3	Безопасность информационных систем	- Угрозы информационной безопасности - Методы защиты информации - Законодательные акты в области информационной безопасности
4.	Управление информационными ресурсами	- Основные принципы управления информационными ресурсами - Методы обеспечения доступности информации - Анализ и оптимизация информационных процессов
5	Современные тенденции в разработке информационных систем	- Облачные технологии - Блокчейн и криптовалюты - Искусственный интеллект в информационных системах
6	Управление	- Методики управления проектами

	проектами в области информационных технологий	- Планирование и контроль проекта - Роль команды разработчиков
7	Интеграция информационных систем	- Принципы совместной работы различных систем - Технологии интеграции данных - Преимущества и недостатки интеграции систем
8	Анализ и оптимизация производительности информационных систем	- Инструменты для мониторинга производительности - Оптимизация работы баз данных - Устранение узких мест в архитектуре системы
9	Резервное копирование и восстановление данных	- Виды резервного копирования - Планирование и автоматизация процесса бэкапа - Восстановление данных после сбоев
10.	Этика и законность в информационных системах	- Законы и нормативные акты в области информационной безопасности - Этические вопросы использования информации - Защита персональных данных
11.	Стратегия развития информационных систем	- Оценка потребностей и меры эффективности ИС - Планирование будущих изменений и обновлений - Разработка стратегии апгрейда информационных систем
12.	Защита информации от внешних и внутренних угроз	- Угрозы со стороны злоумышленников - Внутренние угрозы и утечки данных - Методы защиты от атак и недобросовестных действий.

6.2.2. Содержание практических занятий

№ п/п	**Наименование темы (раздела) дисциплины**	**Содержание практического занятия**
1.	Введение в информационные системы	1. Анализ информационных потребностей организации 2. Построение схем информационного взаимодействия 3. Разработка информационной модели системы 4. Проектирование базы данных
2.	Методы и технологии разработки информационных систем	1. Создание прототипа интерфейса пользователя 2. Разработка архитектуры информационной системы 3. Написание технического задания на разработку ИС 4. Тестирование разработанных модулей
3.	Безопасность информационных систем	1. Оценка уровня информационной безопасности системы 2. Разработка политики безопасности 3. Использование криптографических методов защиты данных 4. Анализ логов системы на предмет угроз
4.	Управление информационными ресурсами	1. Разработка плана управления информационными ресурсами 2. Создание системы мониторинга доступности информации

		3. Анализ процессов обработки информации в организации 4. Оптимизация работы информационных систем
5.	Современные тенденции в разработке информационных систем	1. Создание и настройка облачного хранилища данных 2. Разработка смарт-контрактов на блокчейне 3. Использование машинного обучения для анализа данных 4. Применение нейронных сетей в информационных системах
6.	Управление проектами в области информационных технологий	1. Создание плана проекта 2. Распределение задач в команде разработчиков 3. Мониторинг выполнения задач и контроль сроков 4. Проведение ретроспективных собраний по завершению проекта
7.	Интеграция информационных систем	1. Настройка API для взаимодействия между системами 2. Импорт и экспорт данных между различными базами 3. Использование ETL-процессов для интеграции информации 4. Тестирование целостности данных после интеграции систем
8.	Анализ и оптимизация производительности информационных систем	1. Мониторинг нагрузки на сервера и базы данных 2. Оптимизация SQL-запросов для повышения скорости работы 3. Анализ проблем производительности и поиск их решений 4. Проведение load-тестирования системы
9.	Резервное копирование и восстановление данных	1. Настройка регулярного резервного копирования баз данных 2. Тестирование процедуры восстановления из резервной копии 3. Создание плана действий при потере данных 4. Использование облачных сервисов для хранения бэкапов
10.	Этика и законность в информационных системах	1. Анализ законодательства о защите информации 2. Разработка политики конфиденциальности в организации 3. Проведение аудита безопасности информационной системы 4. Обучение сотрудников правилам безопасного обращения с данными
11.	Стратегия развития информационных систем	1. Составление долгосрочного плана развития информационных систем 2. Анализ потенциальных улучшений и инноваций в ИС 3. Оценка рисков и выгод от проведения изменений 4. Презентация и обсуждение стратегии развития с руководством организации
12.	Защита информации от внешних и внутренних угроз	1. Проведение пенетрационного тестирования системы на предмет уязвимостей 2. Детекция и предотвращение утечек данных 3. Обучение сотрудников правилам безопасной работы с информацией 4. Организация мониторинга и реагирования на инциденты информационной безопасности

6.2.3. Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание самостоятельного занятия
1.	Введение в информационные системы	- Подробнее изучить методы криптографии и шифрования информации. - Изучить основные принципы аутентификации и авторизации пользователей. - Провести исследование по защите информации на различных уровнях сети. - Изучить основные виды угроз информационной безопасности и способы их предотвращения.
2.	Методы и технологии разработки информационных систем	- Изучить особенности сетевых механизмов защиты информации. - Провести исследование по методам детекции и предотвращения вторжений. - Изучить принципы работы брандмауэров и средств защиты от DDoS-атак. - Пройти курс по пентестированию для оценки уровня безопасности информационных систем.
3.	Безопасность информационных систем	- Изучить методику оценки рисков информационной безопасности. - Подробнее изучить процедуры реагирования на инциденты и меры по их предотвращению. - Изучить стандарты ISO/IEC 27001 и ISO/IEC 27002 в области управления информационной безопасностью. - Провести анализ уязвимостей информационных систем и разработать сценарии их эксплуатации.
4.	Управление информационными ресурсами	- Ознакомиться с основными законодательными актами о защите информации и персональных данных. - Провести исследование требований к обработке персональных данных и механизмов защиты конфиденциальной информации. - Изучить процедуры расследования инцидентов информационной безопасности и правовые аспекты их разрешения. - Исследовать международные стандарты и положения GDPR в области защиты данных.
5.	Современные тенденции в разработке информационных систем	- Подробнее изучить специфику работы антивирусов и антиспайваров. - Изучить принципы работы прокси-серверов и сертификацию HTTPS трафика. - Провести сравнительный анализ средств обнаружения угроз и предотвращения атак. - Изучить особенности защиты мобильных устройств и разработать стратегию их обеспечения безопасностью.
6.	Управление проектами в области информационных технологий	- Изучить процедуры проведения аудита информационной безопасности и методики его оценки. - Провести практическое исследование аудиторских отчетов и выявить основные недостатки в защите информации.

		- Изучить методику планирования аудита систем безопасности и его документирования. - Принять участие в симуляции аудита информационной безопасности и разработать рекомендации по устранению выявленных проблем.
7.	Интеграция информационных систем	- Изучить процедуру сертификации информационной безопасности по международным стандартам. - Подробнее ознакомиться с требованиями стандартов ISO/IEC 27001, PCI DSS и их применением в практике. - Провести анализ процесса сертификации информационной безопасности в организациях различного масштаба. - Изучить специфику получения сертификатов соответствия стандартам информационной безопасности и их обновления.
8.	Анализ и оптимизация производительности информационных систем	- Провести анализ современных тенденций в области информационной безопасности (IoT, ИИ, облачные технологии). - Изучить методы и инструменты защиты информации от новых видов угроз и атак. - Рассмотреть примеры успешной реализации инновационных решений в области безопасности. - Разработать стратегию внедрения новых технологий и подходов в обеспечении информационной безопасности с учетом текущих тенденций рынка.
9.	Резервное копирование и восстановление данных	- Изучить методы мониторинга сетевого трафика для выявления аномалий и инцидентов безопасности. - Провести анализ инцидентов информационной безопасности и разработать план действий для их управления. - Изучить процедуры реагирования на инциденты, включая расследование, устранение уязвимостей и восстановление системы. - Принять участие в тренировках и симуляциях по управлению инцидентами информационной безопасности.
10.	Этика и законность в информационных системах	- Изучить методы обучения сотрудников по вопросам информационной безопасности и повышения информационной грамотности. - Разработать образовательные материалы и программы обучения для персонала организации. - Провести тренинги и семинары для сотрудников по правилам обращения с информацией и обеспечению безопасности. - Оценить эффективность проведенного обучения и разработать планы по его совершенствованию.
11.	Стратегия развития информационных систем	- Проанализировать кейсы инцидентов информационной безопасности в различных организациях. - Выявить основные причины и последствия инцидентов, а также уроки, которые можно извлечь из прошлого опыта. - Провести собственный кейс-анализ инцидента информационной безопасности, разработать рекомендации по его предотвращению.

		- Поделиться результатами кейс-анализа с коллегами и обсудить возможные меры по улучшению безопасности информационной системы.
12.	Защита информации от внешних и внутренних угроз	- Изучить особенности защиты данных и обеспечения безопасности в облачных средах. - Провести анализ угроз информационной безопасности при использовании облачных технологий. - Изучить методы шифрования, контроля доступа и мониторинга в облачных средах. - Разработать стратегию безопасности для работы с облачными ресурсами и услугами.

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 информационные системы	Опрос, тестирование.
2	Методы и технологии разработки информационных систем	Опрос, тестирование.
3	Безопасность информационных систем	Опрос, тестирование.
4	Управление информационными ресурсами	Опрос, информационный проект, тестирование.
5	Современные тенденции в разработке информационных систем	Опрос, информационный проект, тестирование.
6	Управление проектами в области информационных технологий	Опрос, информационный проект, тестирование.
7	Интеграция информационных систем	Опрос, информационный проект, тестирование.
8	Анализ и оптимизация производительности информационных систем	Опрос, информационный проект, тестирование.
9.	Резервное копирование и восстановление данных	Опрос, информационный проект, тестирование.
10	Этика и законность в информационных системах	Опрос, информационный проект, тестирование.
11.	Стратегия развития информационных систем	Опрос, информационный проект, тестирование.
12.	Защита информации от внешних и внутренних угроз	Опрос, информационный проект, тестирование.

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

8.1 Основная учебная литература:

1. Бычков, А. А. Надежность информационных систем : учебное пособие / А. А. Бычков. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2024. — 135 с. — ISBN 978-5-9275-4794-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146903.htm
2. Васильев, Р. Б. Управление развитием информационных систем : учебник / Р. Б. Васильев, Г. Н. Калянов, Г. А. Левочкина. — 5-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 507 с. — ISBN 978-5-4497-1654-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/160033.html
3. Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128393.html

8.2. Дополнительная учебная литература

1. Куклина, И. Г. Методы и средства проектирования информационных систем: учебное пособие / И. Г. Куклина, К. А. Сафонов. — Нижний Новгород: Нижегородский государственный архитектурно-строительный университет, ЭБС АСВ, 2020. — 84 с. — ISBN 978-5-528-00419-8. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/107378.html
2. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 263 с. — ISBN 978-5-4497-0666-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97553.html
3. Нестеров, С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 250 с. — ISBN 978-5-4497-2435-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133918.html

8.3. Периодические издания

1. Экономика и менеджмент систем управления [Электронный ресурс] - http://www.iprbookshop.ru/34060.html
2. Экономика и современный менеджмент: теория и практика[Электронный ресурс] - http://www.iprbookshop.ru/48512.html
3. Российский экономический журнал [Электронный ресурс] http://www.iprbookshop.ru/45530.html

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины (модуля)

1. Библиотека материалов по экономической тематик [Электронный ресурс]– https://www.libertarium.ru/library
2. Материалы по социально-экономическому положению и развитию в России [Электронный ресурс]–http://www.finansy.ru
3. Мониторинг экономических показателей [Электронный ресурс]– http://www.budgetrf.ru
4. Официальный сайт Центрального банка России [Электронный ресурс]– http://www.cbr.ru
5. РосБизнесКонсалтинг [Электронный ресурс]–http://www.rbc.ru
6. Росстат [Электронный ресурс]– http:// www.gks.ru
7. Журнал «Вопросы экономики» [Электронный ресурс]–http://vopreco.ru
8. Журнал «Банковское дело» [Электронный ресурс]–http://www.bankdelo.ru
9. Журнал «Финансы и экономика» [Электронный ресурс]–http://finans.rusba.ru
10. Журнал «Эксперт» [Электронный ресурс] – http://www.expert.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:

- работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
- внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов;
- выполнение самостоятельных практических работ;
- подготовка к экзаменам 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 рекомендуется соблюдать следующие правила:

1. Подготовка к экзамену должна проводиться систематически, в течение всего семестра.
2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.
3. 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 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);

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, колонки, проектор, экран.

Перечень лицензионного программного обеспечения, в том числе отечественного производства: Windows 10, КонсультантПлюс, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Yandex Browser, пакет LibreOffice, МТС Линк, Gimp, FreeCAD.

1) IDE Visual Studio Community (нагрузка «Разработка классических приложений на C++» с компонентом «Поддержка C++/CLI»; поддержка MFC)

2) СУБД MySQL (клиент-серверная)

3) Ramus Modelio

4) Cisco Packet Tracer (версии 7.x и 8.x)

5) Oracle Virtual Box

6) Adobe Reader

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 10, КонсультантПлюс, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Adobe Reader, Yandex Browser, пакет LibreOffice, МТС Линк, Gimp, FreeCAD.

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. <u>В освоении учебной дисциплины используются следующие традиционные образовательные технологии:</u>

- 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. <u>Активные и интерактивные методы и формы обучения</u>

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. <u>Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)</u>

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

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

студентов-инвалидов и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Приложение

Автономная некоммерческая организация высшего образования

«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Разработка, сопровождение и обеспечение безопасности информационных систем

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

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-2

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-2	**ПК-2.** Способен использовать математический аппарат и современные компьютерные средства для выполнения научно-исследовательских работ по закрепленной тематике	**ПК-2.3.** Способен использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве. **ПК-2.4.** Собирает и анализирует информацию по решаемой задаче, составляет ее математическое описание, обеспечивает накопление, анализ и систематизацию собранных данных с использованием современных достижений науки и информационных систем; **ПК-2.5.** Выявляет и формулирует актуальные научные проблемы; обосновывать актуальность, теоретическую и практическую значимость темы научного исследования, разрабатывать план и программу проведения научного исследования;

3. Описание планируемых результатов обучения по дисциплине

3.1. <u>Описание планируемых результатов обучения по дисциплине</u>

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

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-2**		
	Основы операционных систем: Знать архитектуру и основные компоненты	Конфигурировать операционные системы: Уметь устанавливать и	Практическими навыками конфигурирования: Владеть навыками

	операционных систем (например, Windows, Linux). Знать принципы работы файловых систем и управления процессами. Сетевые протоколы: Знать основные сетевые протоколы (TCP/IP, HTTP, HTTPS, FTP) и их функции. Знать принципы работы сетевых устройств (маршрутизаторов, коммутаторов, брандмауэров). Инструменты конфигурирования: Знать инструменты и утилиты для конфигурирования операционных систем и сетевых устройств (например, командная строка, PowerShell, SSH). Безопасность: Знать основные принципы и методы обеспечения безопасности операционных систем и сетевых устройств.	настраивать операционные системы для веб-разработки. Уметь управлять пользователями и правами доступа в операционных системах. Настраивать сетевые устройства: Уметь конфигурировать маршрутизаторы и коммутаторы для обеспечения сетевой связности. Уметь настраивать брандмауэры для защиты веб-приложений. Использовать инструменты командной строки: Уметь использовать командную строку для выполнения задач администрирования и конфигурирования. Уметь применять скрипты для автоматизации процессов конфигурирования. Обеспечивать безопасность систем: Уметь применять методы шифрования и аутентификации для защиты данных. Уметь проводить аудит безопасности и выявлять уязвимости в системах.	установки и настройки операционных систем в средах веб-разработки. Владеть навыками конфигурирования сетевых устройств для оптимизации работы веб-приложений. Работой с документацией: Владеть умением читать и интерпретировать техническую документацию по операционным системам и сетевым устройствам. Решением проблем: Владеть навыками диагностики и устранения неполадок в операционных системах и сетевых устройствах. Работой в команде: Владеть навыками взаимодействия с другими специалистами (разработчиками, системными администраторами) для эффективного конфигурирования и поддержки веб-приложений.

3.2. <u>Критерии оценки результатов обучения по дисциплине</u>

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		
НЕУДОВЛЕТВОРИТЕЛЬНО/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.

При подготовке ответа в рамках прохождения промежуточной аттестации (зачет/ зачет с оценкой/ экзамен) обучающимся разрешается использовать калькулятор и справочные таблицы.

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

Тестирование
ПК-2
8 СЕМЕСТР

Разработка, сопровождение и обеспечение безопасности информационных систем

1. Дополните предложение: ... - это совокупность одного или нескольких компьютеров, при необходимости сетевой среды и периферийного оборудования, а также программного обеспечения, организованная для обработки информации. Укажите термин:

Ответ: вычислительная система

2. ... сигнала – это процесс создания информационного сигнала на основе битовой последовательности кадра (фрейма). Укажите название процесса.

Ответ: кодирование

Возможный вариант ответа: кодирование сигнала

3. Общепринятое обозначение распределенной атаки отказа в обслуживании (английская аббревиатура):

Ответ: DDoS

Возможный вариант ответа: DDoS-атака

4. ... - это получение доступа к информации с нарушением правил, установленных законодательством или владельцем.

Ответ: несанкционированный доступ

5. Защита доступа к данным в БД осуществляется прикладным ПО, относящимся к категории:

Ответ: СУБД

Возможный вариант ответа: системы управления базами данных

Возможный вариант ответа: система управления базами данных

6. Архитектура распределенных информационных систем с централизованным доступом к общему ресурсу:

Ответ: клиент-сервер

Возможный вариант ответа: клиент-серверная

Возможный вариант ответа: клиент-серверная архитектура

7. В современных интегрированных сетях наиболее востребованным методом взаимодействия гетерогенных сетей является:

Ответ: туннелирование

Возможный вариант ответа: инкапсуляция

8. Компьютерные программы или устройства для захвата и анализа трафика (например, Wireshark) относятся к категории:

Ответ: сниффер

Возможный вариант ответа: sniffer

Возможный вариант ответа: снифферы

Возможный вариант ответа: sniffers

9. Компоненты вычислительных сетей, для которых определены функциональные роли клиента и сервера:

A. Программные процессы на узлах

B. Каналы связи (среды передачи)

C. Информационные сообщения

D. Сетевые интерфейсы

Ответ: A. Программные процессы на узлах

10. Примеры активных угроз (изменяющих структуру и содержание компонентов информационной системы):

A. несанкционированный доступ

B. вымогатель-шифровальщик файлов

C. IP-спуффинг

D. отказ в обслуживании

Ответ: B. вымогатель-шифровальщик файлов; C. IP-спуффинг

11. Выберите комбинированные типы сетевых атак:

A. sniffing

B. атака эксплойтом

C. атака доступа DoS

D. сетевая разведка

Ответ: B. атака эксплойтом; D. сетевая разведка

12. Выберите задачи ОС по управлению программной (операционной средой):

A. управление с помощью драйверов

B. диспетчеризация программных процессов

C. синхронизация процессов по отношению к общим ресурсам вычислительной системы

D. сетевое взаимодействие

Ответ: B. диспетчеризация программных процессов; C. синхронизация процессов по отношению к общим ресурсам вычислительной системы

13. Для ОС уровневой (слоевой) архитектуры характерно:

A. прикладная программа может получить доступ к оборудованию только посредством ядра ОС

B. временная предсказуемость вычислительной системы в условиях однозадачности

C. прикладная программа может получить доступ к оборудованию различными способами, в т.ч. и непосредственно

D. стабильность работы в условиях многозадачности

Ответ: B. временная предсказуемость вычислительной системы в условиях однозадачности; C. прикладная программа может получить доступ к оборудованию различными способами, в т.ч. и непосредственно

14. К методу синхронизации процессов с блокировкой в ОС относятся приёмы:

A. алгоритм Петерсона

B. блокирование шины памяти

C. семафор Дейкстры

D. мьютекс

Ответ: C. семафор Дейкстры; D. Мьютекс

15. ... - это два или более программных процесса, выполняющиеся на разных узлах, посредством информационного взаимодействия по сети реализующих общую вычислительную задачу (оказание услуги потребителю - пользователю или другой программе).

A. протокольный стек

B. локальная программная служба

C. сетевая программная служба

D. сетевой интерфейс

Ответ: C. сетевая программная служба

16. Откуда происходит захват трафика сниффером типа Wireshark?

A. протокольный порт
B. буфер DNS-клиента
C. буфер сетевой карты
D. файл подкачки ОС

Ответ: C. буфер сетевой карты

17. Средства защиты данных от несанкционированного доступа (ACL) присутствуют в файловых системах:

A. ext4
B. NTFS
C. FAT32
D. HPFS

Ответ: A. ext4; B. NTFS

18. ... - это процедура распознавания субъекта ИС по его идентификатору при попытке субъекта войти в систему.

Ответ: идентификация
Возможный вариант ответа: **идентификация субъекта**
Возможный вариант ответа: **идентификация субъекта ИС**
Возможный вариант ответа: **идентификация субъекта информационной системы**

19. На легковерности пользователя основана сетевая угроза:

Ответ: Phishing
Возможный вариант ответа: Фишинг

20. ... - это процедура проверки подлинности идентифицированного субъекта ИС.

Ответ: аутентификация
Возможный вариант ответа: **аутентификация субъекта**
Возможный вариант ответа: **аутентификация субъекта ИС**
Возможный вариант ответа: **аутентификация субъекта информационной системы**

Типовые вопросы

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое криптографические методы защиты информации?
9. Перечислите виды защищаемой информации.
10. Какие основные законы в области защиты информации в РФ?
11. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
12. Что такое профессиональная тайна?
13. Что такое коммерческая тайна?
14. Что такое государственная тайна?

15. Опишите правовой режим государственной тайны.

Темы исследовательских, творческих проектов

Подготовка исследовательских проектов по темам:

1. Методы противодействия сниффингу.
2. Средства и методы защиты информации от утечки в телефонных линиях.
3. Виды сигнализаций устанавливаются для обеспечения инженерной защиты.
4. Основные стандарты РФ в области информационной безопасности.
5. Российские и международные стандарты на формирование цифровой подписи.

Информационный проект

Подготовьте информационный проект (презентацию) по теме:

1. Инфраструктура открытых ключей.
2. Модели безопасности.
3. Виды защищаемой информации.
4. Организационное обеспечение информационной безопасности.
5. Инженерная защита и охрана объектов.

Творческое задание (с элементами эссе)

Напишите эссе по теме:

1. Основные криптографические протоколы, используемые в сетях.
2. Средства стеганографической защиты информации.
3. Программно-аппаратных средства защиты информации.
4. Основные международные стандарты в области информационной безопасности.
5. Криптографические методы защиты информации.

Типовые вопросы для промежуточной аттестации

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое криптографические методы защиты информации?
9. Перечислите виды защищаемой информации.
10. Какие основные законы в области защиты информации в РФ?
11. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
12. Что такое профессиональная тайна?
13. Что такое коммерческая тайна?
14. Что такое государственная тайна?
15. Опишите правовой режим государственной тайны.
16. Как связаны международные стандарты и стандарты РФ?
17. Что такое политика безопасности?
18. Что такое инженерная защита объектов?

19. Что такое технические каналы утечки информации?
20. Перечислите основные виды технических каналов утечки информации?
21. Перечислите методы защиты информации от утечки по визуальному каналу.
22. Перечислите методы защиты информации от утечки по воздушному каналу.
23. Перечислите методы защиты информации от утечки по вибрационному каналу.
24. Перечислите методы защиты информации от утечки по индукционному каналу.
25. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
26. Что такое брандмауэр?
27. Что такое антивирусная программа?
28. Что такое эвристический алгоритм поиска вирусов?
29. Что такое сигнатурный поиск вирусов?
30. Что такое механизм контроля и разграничения доступа?
31. Что такое криптография?
32. Какие используются симметричные алгоритмы шифрования?
33. Какие используются асимметричные алгоритмы шифрования?
34. Что такое цифровая подпись?
35. Что такое инфраструктура открытых ключей?