Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Кибербезопасность и защита данных

Направление подготовки	Информатика и вычислительная техника
Код	09.03.01
Направленность (профиль)	Автоматизированные системы обработки информации и управления
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-1
Профессиональные	-	ПК-3

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-1	**ПК-1.** Способен к разработке требований к программному обеспечению и комплекта проектной документации информационных систем в соответствии с требованиями нормативно-технической документации	**ПК-1.1.** Знает методы представления данных и разработки основного алгоритма и комплекса программ; тестирования и верификации процедур обработки данных **ПК-1.2.** Умеет составлять комплект проектной документации информационных систем: технического задания, технического предложения, эскизного проекта, технического и рабочего проектов **ПК-1.3.** Владеет навыками выполнения мероприятий контроля соответствия технологических требований и инновационных предложений при разработке программного обеспечения
ПК-3	**ПК-3.** Способен управлять проектами в области информационных технологий на основе полученных планов проектов, поддерживать процессы разработки и модернизации	**ПК-3.1.** Знает первоначальные требования к ИС, перечень и последовательность работ, план мероприятий по управлению разработкой программного обеспечения, определение ресурсов, объемов работ по продвижению IT-продуктов **ПК-3.2.** Умеет проводить разработку архитектуры и прототипов информационных систем, их проектирование и дизайн, обеспечение кодирования на языках программирования, создавать пользовательскую документацию **ПК-3.3.** Владеет навыками проведения валидации программных продуктов и информационных систем, их интеграция с использованием инновационных аналитических методик

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-1**		
	- математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации; - основные идеи, понятия и методы, определяющие стиль написания, отладки и сопровождения программ; - характеристики основных парадигм программирования;	- использовать математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации; - применять современные компьютерные технологии для решения практических задач; - делать обоснованный выбор инструментария для решения прикладных задач;	- навыками использования математического аппарата, методологии программирования и современных компьютерных технологий для решения практических задач получения, хранения, обработки и передачи информации; - математическим аппаратом для построения вычислительных моделей практических задач; - навыками использования стандартных алгоритмических моделей для решения задач хранения и обработки информации
Код компетенции	**ПК-2**		

	Основы операционных систем: Знать архитектуру и основные компоненты 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.	Конфигурировать операционные системы: Уметь устанавливать и 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.	Практическими навыками конфигурирования: Владеть навыками 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.

Код компетенции	ПК-3		
	- Знать основы математического аппарата Понимать ключевые математические концепции и методы, используемые для решения задач в области обработки информации, такие как алгебра, статистика и дискретная математика. - Знать методологию программирования Осознавать основные принципы и парадигмы программирования, включая объектно-ориентированное, функциональное и процедурное программирование. - Знать современные компьютерные технологии Иметь представление о современных технологиях и инструментах для работы с данными, таких как базы данных, облачные решения и языки программирования.	- Уметь применять математические методы Способность использовать математические модели и алгоритмы для решения практических задач, связанных с получением и обработкой информации. - Уметь разрабатывать программные решения Умение создавать программное обеспечение для автоматизации процессов получения, хранения и обработки данных с использованием различных языков программирования. - Уметь работать с компьютерными технологиями Способность эффективно использовать современные инструменты и технологии для управления данными, включая системы управления базами данных (СУБД) и средства визуализации данных.	- Владеть навыками программирования Умение писать код на нескольких языках программирования (например, Python, Java, C++) для решения задач обработки информации. - Владеть инструментами анализа данных Освоение специализированных программных средств для анализа, обработки и визуализации данных, таких как Excel, R или Tableau. - Владеть навыками проектирования систем Умение разрабатывать архитектуру информационных систем, учитывая требования к получению, хранению и передаче информации.

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: Автоматизированные системы обработки информации и управления

5. Объем дисциплины

Виды учебной работы	*Формы обучения*
	Очно-заочная
Общая трудоемкость: зачетные единицы/часы	4/144
Контактная работа:	
Занятия лекционного типа	8
Занятия семинарского типа	12
Промежуточная аттестация: **экзамен**	88
Самостоятельная работа (СРС)	36

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	1			1			12
2.	Средства защиты от вредоносного ПО и доверенной загрузки	1			1			12
3.	Межсетевые экраны и системы предотвращения вторжений	1			2			12
4.	Мониторинг и анализ защищённости	1			2			13
5.	Изолированные среды и виртуализация	1			2			13

6.	Криптографическая защита и резервное копирование	1			2			13
7.	Защита операционных систем и систем ИИ	2			2			13
	Промежуточная аттестация	**36**						
	Итого	**8**			**12**			**88**

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 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).

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

Кибербезопасность и защита данных

Направление подготовки	Информатика и вычислительная техника
Код	09.03.01
Направленность (профиль)	Автоматизированные системы обработки информации и управления
Квалификация выпускника	бакалавр

Москва
2026

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-1
Профессиональные	-	ПК-3

2. **Компетенции и индикаторы их достижения**

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-1	**ПК-1.** Способен к разработке требований к программному обеспечению и комплекта проектной документации информационных систем в соответствии с требованиями нормативно-технической документации	**ПК-1.1.** Знает методы представления данных и разработки основного алгоритма и комплекса программ; тестирования и верификации процедур обработки данных **ПК-1.2.** Умеет составлять комплект проектной документации информационных систем: технического задания, технического предложения, эскизного проекта, технического и рабочего проектов **ПК-1.3.** Владеет навыками выполнения мероприятий контроля соответствия технологических требований и инновационных предложений при разработке программного обеспечения
ПК-3	**ПК-3.** Способен управлять проектами в области информационных технологий на основе полученных планов проектов, поддерживать процессы разработки и модернизации	**ПК-3.1.** Знает первоначальные требования к ИС, перечень и последовательность работ, план мероприятий по управлению разработкой программного обеспечения, определение ресурсов, объемов работ по продвижению IT-продуктов **ПК-3.2.** Умеет проводить разработку архитектуры и прототипов информационных систем, их проектирование и дизайн, обеспечение кодирования на языках программирования, создавать пользовательскую документацию **ПК-3.3.** Владеет навыками проведения валидации программных продуктов и информационных систем, их интеграция с использованием инновационных аналитических методик

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-1**		
	- математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации; - основные идеи, понятия и методы, определяющие стиль написания, отладки и сопровождения программ; - характеристики основных парадигм программирования;	- использовать математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации; - применять современные компьютерные технологии для решения практических задач; - делать обоснованный выбор инструментария для решения прикладных задач;	- навыками использования математического аппарата, методологии программирования и современных компьютерных технологий для решения практических задач получения, хранения, обработки и передачи информации; - математическим аппаратом для построения вычислительных моделей практических задач; - навыками использования стандартных алгоритмических моделей для решения задач хранения и обработки информации
Код компетенции	**ПК-2**		
	Основы операционных систем: Знать архитектуру и основные компоненты операционных систем (например, Windows,	Конфигурировать операционные системы: Уметь устанавливать и настраивать операционные системы для веб-разработки.	Практическими навыками конфигурирования: Владеть навыками установки и

	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.	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.	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.
Код компетенции	**ПК-3**		

	- Знать основы математического аппарата Понимать ключевые математические концепции и методы, используемые для решения задач в области обработки информации, такие как алгебра, статистика и дискретная математика. - Знать методологию программирования Осознавать основные принципы и парадигмы программирования, включая объектно-ориентированное, функциональное и процедурное программирование. - Знать современные компьютерные технологии Иметь представление о современных технологиях и инструментах для работы с данными, таких как базы данных, облачные решения и языки программирования.	- Уметь применять математические методы Способность использовать математические модели и алгоритмы для решения практических задач, связанных с получением и обработкой информации. - Уметь разрабатывать программные решения Умение создавать программное обеспечение для автоматизации процессов получения, хранения и обработки данных с использованием различных языков программирования. - Уметь работать с компьютерными технологиями Способность эффективно использовать современные инструменты и технологии для управления данными, включая системы управления базами данных (СУБД) и средства визуализации данных.	- Владеть навыками программирования Умение писать код на нескольких языках программирования (например, Python, Java, C++) для решения задач обработки информации. - Владеть инструментами анализа данных Освоение специализированных программных средств для анализа, обработки и визуализации данных, таких как Excel, R или Tableau. - Владеть навыками проектирования систем Умение разрабатывать архитектуру информационных систем, учитывая требования к получению, хранению и передаче информации.

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

9 СЕМЕСТР
ПК-1

1. Какой механизм обеспечивает целостность данных при передаче по сети?
а) Симметричное шифрование
б) Электронная подпись (хеш-функция)

в) Сжатие данных
г) Установка антивируса
Правильный ответ: б

2. Как называется атака, при которой злоумышленник перехватывает и изменяет передаваемые данные без ведома отправителя и получателя?
а) Отказ в обслуживании (DoS)
б) Атака «человек посередине» (Man-in-the-Middle)
в) Фишинг
г) Сниффинг
Правильный ответ: б

3. Какой тип сертификатов используется для аутентификации веб-сайтов и установления защищённого соединения по протоколу HTTPS?
а) SSL/TLS-сертификаты (X.509)
б) PGP-сертификаты
в) Самоподписанные сертификаты без проверки
г) Kerberos-билеты
Правильный ответ: а

4. Что такое «белый список» приложений в политике безопасности?
а) Перечень программ, которые запрещены к запуску
б) Перечень программ, которым разрешён запуск, а все остальные блокируются
в) Список обновлений для антивируса
г) Перечень пользователей, имеющих доступ к логам
Правильный ответ: б

5. Какой протокол используется для централизованной аутентификации, авторизации и учёта доступа (AAA) в сетях?
а) RADIUS
б) SNMP
в) SMTP
г) ICMP
Правильный ответ: а

6. Что такое «песочница» (sandbox) в контексте защиты от вредоносного ПО?
а) Изолированная среда для безопасного исполнения подозрительных программ
б) Облачное хранилище для резервных копий
в) Аппаратный модуль шифрования
г) Антивирусная база данных
Правильный ответ: а

7. Какой стандарт описывает систему управления информационной безопасностью (СУИБ)?
а) ISO/IEC 27001
б) IEEE 802.11
в) RFC 1918
г) ГОСТ Р 34.10
Правильный ответ: а

8. Что такое «инъекция SQL»?
а) Метод внедрения вредоносного кода в SQL-запрос через нефильтрованные входные данные

б) Способ шифрования базы данных
в) Процесс оптимизации запросов к СУБД
г) Метод резервного копирования таблиц
Правильный ответ: а

9. Какой тип биометрической аутентификации считается наиболее надёжным?
а) Распознавание отпечатка пальца
б) Распознавание голоса
в) Сканирование радужной оболочки глаза
г) Распознавание лица
Правильный ответ: в (среди перечисленных — наименьшая вероятность ошибки)

10. Какой метод защиты от DDoS-атак заключается в распределении трафика между несколькими серверами?
а) Балансировка нагрузки (load balancing)
б) Фильтрация IP-адресов
в) Отключение сервера
г) Увеличение пропускной способности канала
Правильный ответ: а

11. Что такое «нулевое доверие» (Zero Trust) в архитектуре безопасности?
а) Доверие только пользователям из внутренней сети
б) Принцип, при котором ни один пользователь или устройство не доверяются по умолчанию, даже внутри периметра
в) Отказ от использования паролей
г) Полное шифрование всех данных на диске
Правильный ответ: б

12. Какой протокол используется для безопасного удалённого управления сетевыми устройствами (защищённый доступ к командной строке)?
а) Telnet
б) SSH
в) HTTP
г) FTP
Правильный ответ: б

13. Что такое «симметричное шифрование»?
а) Использование одного и того же ключа для шифрования и дешифрования
б) Использование пары открытого и закрытого ключей
в) Шифрование без ключа
г) Шифрование только заголовков пакетов
Правильный ответ: а

14. Какой элемент системы защиты предназначен для обнаружения атак на основе сигнатур известных уязвимостей?
а) Сканер уязвимостей
б) Система обнаружения вторжений (IDS) с сигнатурным методом
в) Межсетевой экран с фильтрацией по портам
г) Антивирус с эвристическим анализом
Правильный ответ: б

15. Что такое «социальная инженерия» в контексте информационной безопасности?
а) Технический взлом паролей

б) Психологическое манипулирование людьми для получения конфиденциальной информации
в) Физическое проникновение в серверную
г) Анализ исходного кода программ
Правильный ответ: б

9 СЕМЕСТР
ПК-3

1. Какой документ определяет перечень критических информационных ресурсов организации и уровни их защищённости?
а) Политика безопасности
б) Модель угроз
в) Регламент резервного копирования
г) Инструкция по охране труда
Правильный ответ: б

2. Какой показатель используется для оценки риска информационной безопасности?
а) Вероятность угрозы × величина ущерба
б) Скорость передачи данных
в) Количество установленных антивирусов
г) Размер выделенного бюджета
Правильный ответ: а

3. Какая стадия управления инцидентами следует сразу после обнаружения события?
а) Расследование
б) Локализация и изоляция
в) Устранение последствий
г) Архивация логов
Правильный ответ: б

4. Что такое «остаточный риск» в системе управления рисками?
а) Риск, который был полностью устранён
б) Риск, остающийся после применения всех запланированных мер защиты
в) Риск, который невозможно оценить количественно
г) Риск, связанный с человеческим фактором
Правильный ответ: б

5. Какой закон в РФ регулирует порядок обработки персональных данных?
а) ФЗ № 152 «О персональных данных»
б) ФЗ № 149 «Об информации»
в) ФЗ № 187 «О безопасности критической информационной инфраструктуры»
г) ФЗ № 63 «Об электронной подписи»
Правильный ответ: а

6. Что из перечисленного является объектом оценки соответствия при проведении аттестации объекта информатизации?
а) Квалификация сотрудников
б) Реализованные меры защиты и их эффективность
в) Финансовые показатели компании

г) Количество серверов
Правильный ответ: б

7. Какой метод анализа защищённости имитирует действия реального злоумышленника для выявления уязвимостей?
а) Сканирование портов
б) Пентестинг (тестирование на проникновение)
в) Аудит логов
г) Интервью с сотрудниками
Правильный ответ: б

8. Что такое «план непрерывности бизнеса» (BCP) в контексте ИБ?
а) План восстановления после сбоев и катастроф для поддержания деятельности
б) План увольнения сотрудников
в) План замены оборудования
г) План проведения учений
Правильный ответ: а

9. Какой класс защищённости по требованиям ФСТЭК предъявляется к системам, обрабатывающим государственную тайну наивысшей степени секретности?
а) Класс 1
б) Класс 3
в) Класс «А»
г) Класс «Особой важности»
Правильный ответ: а (в классификации ФСТЭК — 1-й класс защищённости)

10. Как часто рекомендуется проводить переоценку рисков информационной безопасности?
а) Один раз в пять лет
б) Периодически, а также при изменении инфраструктуры или угроз
в) Только после инцидента
г) Ежедневно
Правильный ответ: б

11. Что из перечисленного является основным требованием к политике паролей в организации?
а) Минимальная длина и сложность, регулярная смена
б) Использование одного пароля для всех систем
в) Запись паролей в открытом виде
г) Отсутствие требований к смене
Правильный ответ: а

12. Какая метрика позволяет оценить эффективность работы SOC (центра мониторинга безопасности)?
а) Время обнаружения (MTTD) и время реагирования (MTTR)
б) Количество сотрудников в смене
в) Объём хранимых логов
г) Версия используемого SIEM
Правильный ответ: а

13. Что означает термин «управление уязвимостями»?
а) Процесс поиска, классификации и устранения уязвимостей в системе
б) Установка всех обновлений без тестирования

в) Отключение неиспользуемых служб
г) Найм внешнего аудитора
Правильный ответ: а

14. Какой документ определяет порядок действий сотрудников при обнаружении признаков компьютерной атаки?
а) Регламент реагирования на инциденты
б) Штатное расписание
в) Техническое задание на разработку ПО
г) Устав организации
Правильный ответ: а

15. Какое требование предъявляется к ведению журналов аудита (логов) в системах высокой надёжности?
а) Хранение в течение не менее 1 года и защита от изменений
б) Хранение только на бумажных носителях
в) Автоматическое удаление после 7 дней
г) Доступ к логам для всех сотрудников
Правильный ответ: а