Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Защита информационных систем организаций

Направление подготовки	Информационные системы и технологии
Код	09.03.02
Направленность (профиль)	Проектирование, разработка и сопровождение информационных систем
Квалификация выпускника	бакалавр

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 026443C200E0B15FBB4FC3DAFEDBC09294
Владелец: МАНЮШИС АЛЬГИРДАС ЮОЗО
Действителен: с 03.09.2024 до 03.12.2025

Москва
2023

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-5
Профессиональные	-	ПК-6

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-5	Способен выполнять работы по созданию (модификации) и сопровождению ИС	**ПК-5.1.** Успешное создание новой информационной системы с учетом требований безопасности организации. **ПК-5.2**. Эффективная модификация существующей информационной системы с целью улучшения ее защиты. **ПК-5.3.** Активное участие в сопровождении информационной системы, включая выполнение регулярных обновлений и проверок безопасности. **ПК-5.4** Умение анализировать уязвимости в информационных системах и предлагать соответствующие меры по их устранению. **ПК-5.5** Проведение обучающих мероприятий для сотрудников по вопросам безопасности информационных систем.
ПК-6	Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**ПК-6.1.** Разработка информационных систем, которые автоматизируют задачи организационного управления и бизнес-процессы, с учетом требований безопасности. **ПК-6.2**. Модификация существующих информационных систем для улучшения их функциональности и эффективности в сфере организационного управления. **ПК-6.2**. Успешное управление процессом создания информационной системы, включая планирование, координацию и контроль работы команды разработчиков. **ПК-6.4**. Профессиональное сопровождение информационных систем, автоматизирующих задачи управления и бизнес-процессы, в течение их жизненного цикла. **ПК-6.5**. Компетентное консультирование руководства и сотрудников по вопросам использования информационных систем для организационного управления.

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-5**		
	Основы проектирования информационных систем и их компонентов. Принципы работы современных технологий и методов защиты информации. Требования безопасности, применимые к информационным системам. Методы анализа уязвимостей в информационных системах и их компонентов.	Создавать новые информационные системы с учетом требований безопасности. Модифицировать существующие информационные системы для улучшения их уровня защиты. Сопровождать информационные системы, включая обновление и проверку безопасности. Анализировать уязвимости и проводить соответствующие меры по их устранению.	Навыками проектирования информационных систем с учетом требований безопасности. Навыками анализа уязвимостей в информационных системах и разработки мер по обеспечению их безопасности. Навыками работы с современными технологиями и методами защиты информации. Навыками обучения и консультирования сотрудников по вопросам безопасности информационных систем.
Код компетенции	**ПК-6**		
	Принципы автоматизации бизнес-процессов и организационного управления с использованием информационных систем. Методы и подходы к созданию информационных систем, способных эффективно автоматизировать	Проектировать информационные системы, способные автоматизировать задачи организационного управления и бизнес-процессы. Модифицировать существующие информационные системы для улучшения их функциональности в сфере управления.	Проектирования информационных систем с учетом требований бизнес-процессов и организационного управления. Управления проектами создания и сопровождения информационных систем. Работы с командами разработчиков и

	задачи управления. Технологии разработки информационных систем, обеспечивающих высокую производительность и безопасность. Принципы и методы управления проектами создания и сопровождения информационных систем.	Управлять процессом создания информационных систем, включая планирование, координацию и контроль работы команды разработчиков. Сопровождать информационные системы, автоматизирующие задачи управления, на протяжении их жизненного цикла.	координации их деятельности. Консультирования персонала по вопросам использования информационных систем для организационного управления.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информационных систем организаций» относится к части, формируемой участниками образовательных отношений учебного плана ОПОП, является дисциплиной по выбору.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как «Управление проектами», «Информационные системы и базы данных».

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: проектирование, разработка и сопровождение информационных систем

5. Объем дисциплины

Виды учебной работы	***Формы обучения***
	Очная
Общая трудоемкость: зачетные единицы/часы	2/72
Контактная работа:	
Занятия лекционного типа	18
Занятия семинарского типа	18
Промежуточная аттестация: **экзамен**	0,1
Самостоятельная работа (СРС)	35,9

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. Очная форма обучения

№	Раздел/тема	Виды учебной работы (в часах)

п/п		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1.	Основы информационной безопасности	2		2				1,9
2.	Методы защиты информации	2		2				2
3.	Управление доступом и аутентификация	2		2				4
4.	Защита сетевых систем	2		2				4
5.	Защита информации на уровне приложений	2		2				5
6.	Управление инцидентами информационной безопасности	2		2				5
7.	Защита информации в облачных сервисах	2		2				5
8.	Стандарты и законодательство в области информационной безопасности	2		2				5
9.	Тенденции развития информационной безопасности	2		2				4
	Промежуточная аттестация	**0,1**						
	Итого	**18**		**18**				**35,9**

6.2 Программа дисциплины, структурированная по темам / разделам

6.2.1 Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1.	Основы информационной безопасности	- Введение в информационную безопасность - Основные принципы защиты информации - Угрозы и уязвимости информационных систем
2.	Методы защиты информации	- Классификация методов защиты информации - Криптографические методы защиты - Программные и аппаратные средства защиты информации

3.	Управление доступом и аутентификация	- Ролевая модель доступа - Методы аутентификации пользователей - Механизмы контроля доступа к информации
4.	Защита сетевых систем	- Основные принципы защиты сетей - Методы детекции и предотвращения атак на сети - Защита беспроводных сетей
5.	Защита информации на уровне приложений	- Основные угрозы безопасности приложения. -Методы защиты информации в веб-приложениях - Защита баз данных
6.	Управление инцидентами информационной безопасности	- Организация процесса реагирования на инциденты безопасности - Методы обнаружения и анализа инцидентов - Меры по восстановлению после инцидентов
7.	Защита информации в облачных сервисах	- Основы безопасности облачных сервисов - Управление доступом к данным в облаке - Меры безопасности в облачной среде
8.	Стандарты и законодательство в области информационной безопасности	- Основные международные стандарты в области информационной безопасности - Законы и правовые нормы, регулирующие защиту информации - Соблюдение требований нормативно-правовой базы
9.	Тенденции развития информационной безопасности	- Новейшие методы защиты информации - Инновационные технологии в сфере информационной безопасности - Перспективы развития области информационной безопасности.

6.2.2 Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основы информационной безопасности	- Идентификация потенциальных угроз для организации - Анализ уязвимостей информационных систем - Разработка плана действий по устранению угроз
2.	Методы защиты информации	- Ознакомление с основными принципами шифрования - Практические упражнения по работе с криптографическими алгоритмами - Создание и проверка защищенных сообщений
3.	Управление доступом и аутентификация	- Реализация ролевой модели доступа - Настройка механизмов аутентификации и контроля доступа - Проведение тестирования на безопасность
4.	Защита сетевых систем	- Настройка брандмауэров и средств мониторинга сетевой активности - Проведение упражнений по обнаружению и предотвращению сетевых атак - Защита беспроводных сетей с использованием шифрования.
5.	Защита информации на уровне приложений	- Анализ безопасности веб-приложений с

		применением уязвимостей - Применение методов защиты для защиты баз данных - Проведение тестирования на безопасность приложений
6.	Управление инцидентами информационной безопасности	- Разработка сценариев инцидентов для симуляции - Проведение учебных упражнений по реагированию на инциденты - Анализ действий и разработка плана восстановления.
7.	Защита информации в облачных сервисах	- Настройка правильного управления доступом к облачным данным - Реализация мер безопасности для защиты информации в облачной среде - Аудит облачных сервисов на предмет уязвимостей
8.	Стандарты и законодательство в области информационной безопасности	- Разработка политики безопасности с учетом международных стандартов - Проведение аудита соответствия требованиям законодательства - Обучение сотрудников по вопросам соблюдения правил и нормативов
9.	Тенденции развития информационной безопасности	- Проведение исследований по новейшим методам защиты информации - Разработка инновационных проектов по улучшению информационной безопасности - Презентация проектов и обсуждение их потенциальной реализации.

6.2.3 Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание самостоятельной работы
1.	Основы информационной безопасности	- Изучить современные методы обнаружения угроз информационной безопасности и оценить их эффективность. - Провести анализ случаев успешной защиты информации от угроз и определить ключевые факторы, влияющие на успех. - Провести анализ угроз информационной безопасности в конкретной организации и разработать список потенциальных уязвимостей. - Изучить основные принципы защиты информации и создать план действий по их внедрению. - Ознакомиться с основными типами угроз для информационной безопасности и разработать стратегию противодействия.
2.	Методы защиты информации	-Провести обзор существующих криптографических методов защиты информации и выбрать наиболее эффективные для конкретной ситуации. - Попробовать реализовать шифрование данных с использованием различных алгоритмов и оценить их надежность.

		- Изучить программные и аппаратные средства защиты информации и выбрать наиболее подходящие для решения конкретных задач. - Освоить методы анализа безопасности программного обеспечения и провести аудит безопасности. - Провести исследование в области технологий защиты информации и подготовить доклад о последних тенденциях и инновациях.
3.	Управление доступом и аутентификация	- Изучение методов управления доступом, включая RBAC и ABAC модели, и методов их реализации. - Подробное изучение стандартов аутентификации, таких как OAuth, OpenID и SAML, и применение их на практике. - Обзор методов единой идентификации и синхронизации паролей для обеспечения безопасного доступа к ресурсам.
4.	Защита сетевых систем	- Изучение принципов работы брандмауэров, VPN и систем обнаружения вторжений для обеспечения безопасности сети. - Анализ специфики сетевых атак, таких как межсетевые эксплойты, ARP-подделки и MITM атаки. - Практическое обучение по настройке и мониторингу безопасности сети, включая фильтрацию трафика и создание правил доступа.
5.	Защита информации на уровне приложений	- Изучение основных классов уязвимостей приложений, таких как инъекции, переполнения буфера и CSRF, и методов защиты от них. - Практическое тестирование на проникновение веб-приложений с использованием инструментов, таких как Burp Suite или OWASP ZAP. - Анализ безопасности мобильных приложений и методов защиты конфиденциальной информации на мобильных устройствах.
6.	Управление инцидентами информационной безопасности	- Изучение процедур инцидентного реагирования и разработка плана действий в случае кибератаки или утечки информации. - Практическая тренировка по симуляции киберинцидентов и координации действий команды по восстановлению после атаки. - Изучение методов анализа инцидентов и определения причин возникновения, чтобы в дальнейшем снизить вероятность повторения.
7.	Защита информации в облачных сервисах	- Подробное изучение принципов безопасности облачных вычислений и рисков утечки данных при использовании облачных сервисов. - Практическое обучение по настройке и контролю доступа к данным в облачной среде, включая шифрование данных и мониторинг активности. - Анализ сценариев атак на облачные сервера и разработка мер по защите информации в облачной среде.

8.	Стандарты и законодательство в области информационной безопасности	- Изучение основных международных и национальных стандартов безопасности информации, их требования и принципы реализации. - Подробный анализ законодательства о защите персональных данных и влияния законов на процессы обработки и хранения конфиденциальной информации. - Практическое изучение процедур аудита соответствия стандартам и разработка мероприятий по улучшению безопасности в соответствии с требованиями законодательства.
9.	Тенденции развития информационной безопасности	- Изучение современных тенденций и вызовов в области кибербезопасности, включая новые угрозы, технологии и методы противодействия. - Обзор инновационных решений и новых технологий в области информационной безопасности, таких как блокчейн, искусственный интеллект и машинное обучение. - Практическое исследование и обсуждение последних событий и новостей, связанных с областью информационной безопасности, для поддержания актуальности знаний и навыков.

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, тестирование.
2.	Методы защиты информации	Опрос, проблемно-аналитическое задание, тестирование.
3.	Управление доступом и аутентификация	Опрос, проблемно-аналитическое задание, тестирование.
4.	Защита сетевых систем	Опрос, проблемно-аналитическое задание, тестирование.
5.	Защита информации на уровне приложений	Опрос, проблемно-аналитическое задание, тестирование.
6.	Управление инцидентами информационной безопасности	Опрос, проблемно-аналитическое задание, тестирование.
7.	Защита информации в облачных сервисах	Опрос, проблемно-аналитическое задание, тестирование.

8.	Стандарты и законодательство в области информационной безопасности	Опрос, проблемно-аналитическое задание, тестирование.
9.	Тенденции развития информационной безопасности	Опрос, проблемно-аналитическое задание, тестирование.

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

8.1. Основная учебная литература

1. Бова В.В. Основы проектирования информационных систем и технологий: учебное пособие / Бова В.В., Кравченко Ю.А. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. — 105 с. — ISBN 978-5-9275-2717-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/87462.html

2. Иванова О.Г. Методы и средства проектирования информационных систем и технологий. Основы UML: учебное пособие / Иванова О.Г., Громов Ю.Ю. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2020. — 80 с. — ISBN 978-5-8265-2308-7. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/115768.html

3. Куклина И.Г. Методы и средства проектирования информационных систем: учебное пособие / Куклина И.Г., Сафонов К.А. — 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

4. Токмаков Г.П. CASE-технологии проектирования информационных систем: учебное пособие / Токмаков Г.П. — Ульяновск: Ульяновский государственный технический университет, 2018. — 225 с. — ISBN 978-5-9795-1805-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/106080.html

8.2. Дополнительная учебная литература:

1. Бурков А.В. Проектирование информационных систем в Microsoft SQL Server 2008 и Visual Studio 2008: учебное пособие / Бурков А.В. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 310 с. — ISBN 978-5-4497-0353-8. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/89466.html

2. Кукарцев В.В. Проектирование и архитектура информационных систем: учебник / Кукарцев В.В., Царев Р.Ю., Антамошкин О.А. — Красноярск: Сибирский федеральный университет, 2019. — 192 с. — ISBN 978-5-7638-3620-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/100091.html

8.3. Периодические издания

1. Журнал «Математическое моделирование и численные методы». Математическое моделирование и численные методы (bmstu.ru)
2. Вестник Московского Университета. Математика, Механика (msu.su)
3. Дискретная математика. Discrete Mathematics and Applications. (mathnet.ru)

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 /
4. Электронно-библиотечная система ЛАНЬ https://e.lanbook.com/
3. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru
4. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)
5. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
6. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
7. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)

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. В течение семестра, необходимо подготовить рефераты (проекты) с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

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

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

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

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

3. Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

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

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

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. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:

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

13.2. Активные и интерактивные методы и формы обучения

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

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

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

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее –

инвалиды и лица с ОВЗ) с целью обеспечения их прав. При обучении учитываются особенности их психофизического развития, индивидуальные возможности и при необходимости обеспечивается коррекция нарушений развития и социальная адаптация указанных лиц.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально-технического обеспечения, особенностями восприятия учебной информации студентов-инвалидов и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

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

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

Приложение

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Защита информационных систем организаций

Направление подготовки	Информационные системы и технологии
Код	09.03.02
Направленность (профиль)	Проектирование, разработка и сопровождение информационных систем
Квалификация выпускника	бакалавр

Москва
2023

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

Группа компетенций	Категория компетенций	Код
Профессиональные	-	ПК-5
Профессиональные	-	ПК-6

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-5	Способен выполнять работы по созданию (модификации) и сопровождению ИС	**ПК-5.1.** Успешное создание новой информационной системы с учетом требований безопасности организации. **ПК-5.2**. Эффективная модификация существующей информационной системы с целью улучшения ее защиты. **ПК-5.3.** Активное участие в сопровождении информационной системы, включая выполнение регулярных обновлений и проверок безопасности. **ПК-5.4** Умение анализировать уязвимости в информационных системах и предлагать соответствующие меры по их устранению. **ПК-5.5** Проведение обучающих мероприятий для сотрудников по вопросам безопасности информационных систем.
ПК-6	Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**ПК-6.1.** Разработка информационных систем, которые автоматизируют задачи организационного управления и бизнес-процессы, с учетом требований безопасности. **ПК-6.2**. Модификация существующих информационных систем для улучшения их функциональности и эффективности в сфере организационного управления. **ПК-6.2**. Успешное управление процессом создания информационной системы, включая планирование, координацию и контроль работы команды разработчиков. **ПК-6.4**. Профессиональное сопровождение информационных систем, автоматизирующих задачи управления и бизнес-процессы, в течение их жизненного цикла. **ПК-6.5**. Компетентное консультирование руководства и сотрудников по вопросам использования информационных систем для организационного управления.

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-5**		
	1. Основы проектирования информационных систем и их компонентов. 2. Принципы работы современных технологий и методов защиты информации. 3. Требования безопасности, применимые к информационным системам. 4. Методы анализа уязвимостей в информационных системах и их компонентов.	1. Создавать новые информационные системы с учетом требований безопасности. 2. Модифицировать существующие информационные системы для улучшения их уровня защиты. 3. Сопровождать информационные системы, включая обновление и проверку безопасности. 4. Анализировать уязвимости и проводить соответствующие меры по их устранению.	1. Навыками проектирования информационных систем с учетом требований безопасности. 2. Навыками анализа уязвимостей в информационных системах и разработки мер по обеспечению их безопасности. 3. Навыками работы с современными технологиями и методами защиты информации. 4. Навыками обучения и консультирования сотрудников по вопросам безопасности информационных систем.
Код компетенции	**ПК-6**		
	1. Принципы автоматизации бизнес-процессов и организационного управления с использованием информационных систем. 2. Методы и подходы к созданию информационных систем, способных эффективно	1. Проектировать информационные системы, способные автоматизировать задачи организационного управления и бизнес-процессы. 2. Модифицировать существующие информационные системы для улучшения их	1. Проектирования информационных систем с учетом требований бизнес-процессов и организационного управления. 2. Управления проектами создания и сопровождения информационных систем. 3. Работы с командами

	автоматизировать задачи управления. 3. Технологии разработки информационных систем, обеспечивающих высокую производительность и безопасность. 4. Принципы и методы управления проектами создания и сопровождения информационных систем.	функциональности в сфере управления. 3. Управлять процессом создания информационных систем, включая планирование, координацию и контроль работы команды разработчиков. 4. Сопровождать информационные системы, автоматизирующие задачи управления, на протяжении их жизненного цикла.	разработчиков и координации их деятельности. 4. Консультирования персонала по вопросам использования информационных систем для организационного управления.

3.2. Критерии оценки результатов обучения по дисциплине

Шкала оценивания	**Индикаторы достижения**	**Показатели оценивания результатов обучения**
ОТЛИЧНО/ ЗАЧТЕНО	Знает:	- студент глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- студент умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.
	Владеет:	- студент владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО/ ЗАЧТЕНО	Знает:	- студент твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- студент умеет самостоятельно и в основном правильно решать

		учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя научные понятия и ссылки на нормативную базу.
	Владеет:	- студент в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
УДОВЛЕТВОРИТЕЛЬНО/ ЗАЧТЕНО	Знает:	- студент ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- студент в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- студент владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
Компетенция не достигнута		
НЕУДОВЛЕТВОРИТЕЛЬНО/ НЕ ЗАЧТЕНО	Знает:	- студент не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.
	Умеет:	студент не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым “удовлетворительно”.

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

7 СЕМЕСТР
ПК-5

1. Какой из следующих методов является основным для защиты конфиденциальной информации?
A) Шифрование
B) Архивирование
C) Копирование
D) Удаление
Правильный ответ: A

2. Что такое фишинг?
A) Метод защиты данных
B) Способ кражи личной информации
C) Программное обеспечение для шифрования
D) Вирус, который повреждает файлы
Правильный ответ: B

3. Какой из следующих факторов не относится к угрозам информационной безопасности?
A) Вредоносные программы
B) Человеческий фактор
C) Неправильная конфигурация системы
D) Высокая скорость интернета
Правильный ответ: D

4. Что такое брандмауэр?
A) Программа для шифрования данных
B) Устройство для защиты сети от несанкционированного доступа
C) Метод резервного копирования данных
D) Вредоносное ПО
Правильный ответ: B

5. Какой из следующих типов атак направлен на перегрузку сервера?
A) SQL-инъекция
B) DDoS-атака
C) Фишинг
D) Вредоносное ПО
Правильный ответ: B

6. Что такое VPN?
A) Программа для шифрования файлов
B) Виртуальная частная сеть, обеспечивающая защищенное соединение через интернет
C) Устройство для защиты от вирусов
D) Метод резервного копирования данных
Правильный ответ: B

7. Какой из следующих методов аутентификации является наиболее безопасным?

A) Пароль
B) SMS-код
C) Биометрическая аутентификация
D) Ответ на секретный вопрос
Правильный ответ: C

8. Что такое социальная инженерия в контексте информационной безопасности?
A) Использование программного обеспечения для защиты данных
B) Манипуляция людьми для получения конфиденциальной информации
C) Способ шифрования данных
D) Метод резервного копирования
Правильный ответ: B

9. Какой из следующих типов шифрования считается симметричным?
A) RSA
B) AES
C) ECC
D) Diffie-Hellman
Правильный ответ: B

10. Что такое инцидент безопасности информации?
A) Процесс резервного копирования данных
B) Событие, которое угрожает безопасности информации
C) Метод шифрования данных
D) Программа для анализа уязвимостей
Правильный ответ: B

11. Какова основная цель политики безопасности информации в организации?
A) Увеличение прибыли компании
B) Защита конфиденциальности и целостности данных
C) Обучение сотрудников работе с ПО
D) Оптимизация бизнес-процессов
Правильный ответ: B

12. Что такое уязвимость в контексте информационных систем?
A) Защита от вирусов
B) Слабое место, которое может быть использовано злоумышленником
C) Метод шифрования данных
D) Процесс резервного копирования
Правильный ответ: B

13. Какой из следующих методов не является средством защиты информации?
A) Антивирусное ПО
B) Шифрование данных
C) Регулярное обновление ПО
D) Открытие всех портов на сервере
Правильный ответ: D

14. Что такое "гриф секретности" в контексте информации?
A) Уровень важности информации, определяющий ее защиту
B) Метод шифрования данных
C) Тип вредоносного ПО

D) Процесс резервного копирования
Правильный ответ: A

15. Какой из следующих терминов относится к защите информации во время передачи?
– A) Шифрование
– B) Архивирование
– C) Кэширование
– D) Индексация
– Правильный ответ: A

16. Что такое "вредоносное ПО"?
– A Программа, предназначенная для защиты данных
– B) Программа, которая наносит вред компьютерам или сетям
– C) Метод резервного копирования
– D) Устройство для защиты от вирусов
– Правильный ответ: B

17. Какой из следующих факторов не влияет на безопасность информационных систем?
– A) Обновление программного обеспечения
– B) Использование сложных паролей
– C) Наличие антивируса
– D) Высокая скорость интернета
– Правильный ответ: D

18. Что такое "информационная утечка"?
– A) Процесс резервного копирования
– B) Несанкционированное раскрытие конфиденциальной информации
– C) Метод шифрования данных
– D) Защита от вирусов
– Правильный ответ: B

19. Какой метод используется для предотвращения доступа к системе злоумышленников?
– A) Шифрование данных
– B) Аутентификация пользователей
– C) Архивирование
– D) Кэширование
– Правильный ответ: B

20. Что такое "потеря данных"?
– A) Процесс резервного копирования
– B) Несанкционированное уничтожение или потеря информации
– C) Метод шифрования данных
– D) Защита от вирусов
– Правильный ответ: B

21. Какой из следующих методов используется для анализа уязвимостей системы?
– A) Тестирование на проникновение
– B) Архивирование
– C) Шифрование данных

– D）Кэширование
– Правильный ответ: A

22. Что такое "информационная безопасность"?
– A）Защита информации от несанкционированного доступа и использования
– B）Процесс резервного копирования данных
– C）Метод шифрования файлов
– D）Управление бизнес-процессами
– Правильный ответ: A

23. Какой из следующих стандартов относится к управлению информационной безопасностью?
– A）ISO/IEC 27001
– B）ISO 9001
– C）ISO/IEC 20000
– D）ISO 14001
– Правильный ответ: A

24. Что такое "киберугроза"?
– A）Угроза, связанная с физическим доступом к оборудованию
– B）Угроза, возникающая в результате использования компьютерных технологий
– C）Угроза, связанная с недостатками в бизнес-процессах
– D）Угроза, связанная с недостатками в управлении персоналом
– Правильный ответ: B

25. Какой метод используется для защиты паролей?
– A）Хеширование
– B）Архивирование
– C）Кэширование
– D）Индексация
– Правильный ответ: A

Задания открытого типа

1. Что такое информационная безопасность для организации?
2. Что такое управление доступом?
3. Какие законы регулируют обработку персональных данных?

№ п/п	Вопрос	Ответ
1	Что такое информационная безопасность для организации?	Информационная безопасность для организации — это защита данных и информационных систем от несанкционированного доступа, утечек, потерь, повреждений и других угроз, чтобы обеспечить конфиденциальность, целостность и доступность информации.

2	Что такое управление доступом?	Управление доступом — это процесс контроля, который регулирует, кто и какие ресурсы может использовать в информационных системах, на основе установленных прав и разрешений, с целью защиты информации от несанкционированного доступа.
3	Какие законы регулируют обработку персональных данных?	**Федеральный закон "О персональных данных"** (№ 152-ФЗ). **Федеральный закон "О защите прав потребителей"** (№ 2300-1). **Трудовой кодекс РФ** (в части обработки персональных данных сотрудников). **Гражданский кодекс РФ** (в аспекте правовых норм на обработку данных). **Закон о рекламе** (в части обработки данных для маркетинговых целей).

7 СЕМЕСТР
ПК-6

1. Какой из следующих методов является основным для защиты информации?
A) Шифрование
B) Архивирование
C) Копирование
D) Удаление
Правильный ответ: A

2. Что такое фишинг?
A) Метод защиты данных
B) Способ кражи личной информации
C) Программное обеспечение для шифрования
D) Вирус, который повреждает файлы
Правильный ответ: B

3. Какой из перечисленных факторов не относится к угрозам информационной безопасности?
A) Вредоносные программы
B) Человеческий фактор
C) Неправильная конфигурация системы
D) Высокая скорость интернета
Правильный ответ: D

4. Что такое брандмауэр?
A) Программа для шифрования данных
B) Устройство для защиты сети от несанкционированного доступа
C) Метод резервного копирования данных
D) Вредоносное ПО
Правильный ответ: B

5. Какой из следующих методов аутентификации является наиболее безопасным?
A) Пароль

B) SMS-код
C) Биометрическая аутентификация
D) Ответ на секретный вопрос
Правильный ответ: C

6. Что такое социальная инженерия в контексте информационной безопасности?
A) Использование программного обеспечения для защиты данных
B) Манипуляция людьми для получения конфиденциальной информации
C) Способ шифрования данных
D) Метод резервного копирования
Правильный ответ: B

7. Какой из следующих типов атак направлен на перегрузку сервера?
A) SQL-инъекция
B) DDoS-атака
C) Фишинг
D) Вредоносное ПО
Правильный ответ: B

8. Что такое VPN?
A) Программа для шифрования файлов
B) Виртуальная частная сеть, обеспечивающая защищенное соединение через интернет
C) Устройство для защиты от вирусов
D) Метод резервного копирования данных
Правильный ответ: B

9. Какой из перечисленных методов не является средством защиты информации?
A) Антивирусное ПО
B) Шифрование данных
C) Регулярное обновление ПО
D) Открытие всех портов на сервере
Правильный ответ: D

10. Что такое инцидент безопасности информации?
A) Процесс резервного копирования данных
B) Событие, которое угрожает безопасности информации
C) Метод шифрования данных
D) Программа для анализа уязвимостей
Правильный ответ: B

11. Какой из следующих типов шифрования считается симметричным?
A) RSA
B) AES
C) ECC
D) Diffie-Hellman
Правильный ответ: B

12. Какова основная цель политики безопасности информации в организации?
A) Увеличение прибыли компании
B) Защита конфиденциальности и целостности данных
C) Обучение сотрудников работе с ПО
D) Оптимизация бизнес-процессов

Правильный ответ: B

13. такое уязвимость в контексте информационных систем?
A) Защита от вирусов
B) Слабое место, которое может быть использовано злоумышленником
C) Метод шифрования данных
D) Процесс резервного копирования
Правильный ответ: B

14. Какой из следующих методов не обеспечивает защиту от вирусов?
A) Антивирусное ПО
B) Файрволл (брандмауэр)
C) Шифрование данных
D) Регулярные обновления системы
Правильный ответ: C

15. Что такое "гриф секретности" в контексте информации?
A) Уровень важности информации, определяющий ее защиту
B) Метод шифрования данных
C) Тип вредоносного ПО
D) Процесс резервного копирования
Правильный ответ: A

16. Какой из следующих терминов относится к защите информации во время передачи?
A) Шифрование
B) Архивирование
C) Кэширование
D) Индексация
Правильный ответ: A

17. Что такое "вредоносное ПО"?
A) Программа, предназначенная для защиты данных
B) Программа, которая наносит вред компьютерам или сетям
C) Метод резервного копирования
D) Устройство для защиты от вирусов
Правильный ответ: B

18. Какой из следующих факторов не влияет на безопасность информационных систем?
A) Обновление программного обеспечения
B) Использование сложных паролей
C) Наличие антивируса
D) Высокая скорость интернета
Правильный ответ: D

19. Что такое "информационная утечка"?
A) Процесс резервного копирования
B) Несанкционированное раскрытие конфиденциальной информации
C) Метод шифрования данных
D) Защита от вирусов
Правильный ответ: B

20. Какой из перечисленных методов используется для защиты паролей?

A) Хеширование
B) Архивирование
C) Кэширование
D) Индексация
Правильный ответ: A

21. Что такое "киберугроза"?
A) Угроза, связанная с физическим доступом к оборудованию
B) Угроза, возникающая в результате использования компьютерных технологий
C) Угроза, связанная с недостатками в бизнес-процессах
D) Угроза, связанная с недостатками в управлении персоналом
Правильный ответ: B

22. Какой метод используется для предотвращения доступа к системе злоумышленников?
A) Шифрование данных
B) Аутентификация пользователей
C) Архивирование
D) Кэширование
Правильный ответ: B

23. Что такое "потеря данных"?
A) Процесс резервного копирования
B) Несанкционированное уничтожение или потеря информации
C) Метод шифрования данных
D) Защита от вирусов
Правильный ответ: B

24. Какой из следующих методов используется для анализа уязвимостей системы?
A) Тестирование на проникновение
B) Архивирование
C) Шифрование данных
D) Кэширование
Правильный ответ: A

25. Что такое "информационная безопасность"?
A) Защита информации от несанкционированного доступа и использования
B) Процесс резервного копирования данных
C) Метод шифрования файлов
D) Управление бизнес-процессами
Правильный ответ: A

Задания открытого типа

1. Какие методы защиты существуют от DDoS-атаки?
2. Что такое многофакторная аутентификация?
3. Какие существуют методы защиты информации?

№ п/п	Вопрос	Ответ
1	Какие методы защиты существуют от DDoS-атаки?	Методы защиты от DDoS: фаерволы, IDS/IPS, анти-DDoS сервисы, масштабирование, rate limiting, geo-blocking.
2	Что такое многофакторная аутентификация?	Многофакторная аутентификация — это метод подтверждения личности пользователя, требующий использования двух или более факторов: что-то, что пользователь знает (пароль), что-то, что он имеет (смартфон, токен), или что-то, что он представляет (биометрия).
3	Какие существуют методы защиты информации?	Методы защиты информации: шифрование, аутентификация, управление доступом, резервное копирование, антивирусная защита, физическая безопасность, системы обнаружения вторжений (IDS/IPS), регулярные обновления и патчи.