Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Система информационной безопасности предприятия

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.** Типовое проектирование информационных систем, а также различных моделей информационных систем и проектных спецификаций; Программные прототипы решения прикладных задач. **ПК-5.2.** Разработка ИС с учетом требований заказчика, на основе стандартов к проектированию информационных систем. Модификация существующих ИС для улучшения их функциональности и производительности. **ПК-5.3.** Способность разрабатывать мобильные приложения и работать с Интернет вещами **ПК-5.4.** Знать и уметь работать с технологиями искусственного интеллекта и инструментальными средствами разработки интеллектуальных программных систем. **ПК-5.5.** Верификация структуры программного кода ИС относительно архитектуры ИС. **ПК-5.6.** Создание пользовательские интерфейсы с учетом UX/UI принципов для повышения удобства использования ИС. **ПК-5.7.** Осуществляет поиск, анализ, программную реализацию математических моделей и алгоритмов интеллектуальной обработки данных.
ПК-6	Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.	**ПК-6.1.** Способен управлять процессом создания и модификации информационной системы, включая планирование, контроль выполнения работ, оценку и регулирование рисков. **ПК-6.2.** Владеет современными методами и средствами проектирования и разработки баз данных. **ПК-6.3.** Выполняет установку и настройку специализированных программных средств обеспечения безопасности, настройку параметров безопасности операционных систем сетевых устройств.

		ПК-6.4. Осуществляет поддержку и обслуживание ИС, в том числе решение проблемных ситуаций и устранение ошибок. **ПК-6.5.** Владеет инструментами для управления элементами ИТ-инфраструктуры при внедрении, эксплуатации и сопровождении информационных систем и сервисов. **ПК-6.6.** Интеграция различных компонентов ИС для обеспечения их эффективной работы. **ПК-6.7.** Понимает основы продуктовой разработки, может определить требования к продукту, планировать и управлять его разработкой, а также анализировать и учитывать потребности заказчика и конечных пользователей для достижения высокого уровня удовлетворения от использования продукта.

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. Основные стандарты и нормативы, касающиеся разработки и оформления технической документации в области информационных технологий. 2. Требования к технической документации, предъявляемые к профессионалам в области администрирования информационных систем и проектов. 3. Методы и подходы к структурированию и организации технической документации.	1.Умение составлять техническую документацию (технические задания, инструкции, руководства, отчеты) согласно установленным стандартам. 2. Навык работать с текстовыми и графическими редакторами для подготовки и оформления технической документации. 3. Умение структурировать информацию, делать ее легкодоступной и понятной для целевой аудитории. 4. Навык проведения	Навыками работы с документационными системами и инструментами для разработки технической документации (например, MS Word, Visio, Confluence). 2. Опытом использования шаблонов и стандартов оформления технической документации. 3. Навыками для эффективного взаимодействия с другими участниками проекта по вопросам разработки

	4. Принципы создания пользовательских инструкций и технических руководств. 5. Требования по защите конфиденциальности и безопасности информации в документации. 6. Принципы и методы контроля версий и изменений в технической документации.	анализа и интерпретации требований к технической документации. 5. Умение использовать терминологию и язык, соответствующие целевой аудитории документации. 6. Навык оформления диаграмм, схем и других графических элементов в технической документации.;	технической документации. 4. Умение работать в команде над разработкой согласованной технической документации. 5. Опыт управления временем и приоритетами при создании и обновлении документации. 6. Навык анализа и оценки качества технической документации для ее улучшения и совершенствования.
Код компетенции	**ПК-6**		
	- виды угроз информационных систем и методы обеспечения информационной безопасности; - основы информационной безопасности организации; - параметры безопасности и защиты программного обеспечения сетевых устройств, средства управления и обеспечения безопасности администрируемой сети.	- организовать комплексную защиту информационных систем; - определять параметры безопасности и защиты программного обеспечения сетевых устройств, устанавливать и администрировать средства управления и обеспечения безопасности администрируемой сети; - выполнять контроль использования ресурсов сетевых устройств и программного обеспечения; - оценивать производительность сетевой инфраструктуры инфокоммуникационн	- навыками выполнения регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы, восстановления параметров программного обеспечения сетевых устройств; - средствами контроля использование ресурсов сетевых устройств и программного обеспечения; - методами настройки сетевых элементов инфокоммуникационной системы; - правовыми, административными, программно-

		ой системы и использовать инструменты диагностики отказов и ошибок сетевых устройств.	аппаратными средствами информационной защиты, навыками работы с инструментальными средствами защиты информации.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Система информационной безопасности предприятия» относится к части, формируемой участниками образовательных отношений учебного плана ОПОП, является дисциплиной по выбору.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как «Проектирование информационных систем», «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: **зачет**	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

№ п/п	**Раздел/тема**	**Виды учебной работы (в часах)**						
		Контактная работа						**Самостоятельная работа**
		Занятия лекционного типа		**Занятия семинарского типа**				
		Лекции	*Иные учебные*	*Практические*	*Семинары*	*Лабораторные*	*Иные*	

			занятия	*занятия*		*работы*		
1.	Основные понятия и определения информационной безопасности.	2		2				3
2.	Понятие угрозы. Виды угроз информационной безопасности	2		2				4
3.	Понятия утечки информации.	2		2				4
4.	Криптографические методы защиты.	2		2				4
5.	Технологии аутентификации.	2		2				4
6.	Атаки на сервера и рабочие станции.	2		2				4
7.	Технологии межсетевых экранов.	2		2				3
8.	Антивирусная защита.	2		2				3
9.	Технологии построения защищенных информационных систем.	2		2				3,9
	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.	Основные понятия и определения информационной безопасности.	Проблема информационной безопасности. Виды защищаемой информации.
2.	Понятие угрозы. Виды угроз информационной безопасности	Характеристики информационных атак. Информационная безопасность в условиях функционирования в России глобальных сетей.
3.	Понятия утечки информации.	Основные нарушения. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.
4.	Криптографические методы защиты.	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования. Алгоритмы шифрования. Электронная цифровая подпись.

5.	Технологии аутентификации.	Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли.
6.	Атаки на сервера и рабочие станции.	Атака типа «отказ в обслуживании». Протоколирование. Настройка и использование файрволов.
7.	Технологии межсетевых экранов.	Функции межсетевых экранов и особенности их функционирования. Схемы сетевой защиты на базе межсетевых экранов.
8.	Антивирусная защита.	Объекты внедрения, режимы функционирования и специальные функции вирусов. Основные принципы использования антивирусного программного обеспечения.
9.	Технологии построения защищенных информационных систем.	Средства операционной системы. Средства резервирования данных. Проверка целостности.

6.2.2 Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основные понятия и определения информационной безопасности.	Проблема информационной безопасности. Виды защищаемой информации.
2.	Понятие угрозы. Виды угроз информационной безопасности	Характеристики информационных атак. Информационная безопасность в условиях функционирования в России глобальных сетей.
3.	Понятия утечки информации.	Основные нарушения. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.
4.	Криптографические методы защиты.	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования. Алгоритмы шифрования. Электронная цифровая подпись.
5.	Технологии аутентификации.	Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли.
6.	Атаки на сервера и рабочие станции.	Атака типа «отказ в обслуживании». Протоколирование. Настройка и использование файрволов.
7.	Технологии межсетевых экранов.	Функции межсетевых экранов и особенности их функционирования. Схемы сетевой защиты на базе межсетевых экранов.
8.	Антивирусная защита.	Объекты внедрения, режимы функционирования и специальные функции вирусов. Основные принципы использования антивирусного программного обеспечения.
9.	Технологии построения защищенных информационных систем.	Средства операционной системы. Средства резервирования данных. Проверка целостности.

6.2.3 Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1.	Основные понятия и определения информационной безопасности.	Модели информационной безопасности. Выбор средств защиты системы информационной безопасности
2.	Понятие угрозы. Виды угроз информационной безопасности	Инструменты информационных атак. Средства предупреждения атак.
3.	Понятия утечки информации.	Электромагнитные, электрические и параметрические каналы утечки информации
4.	Криптографические методы защиты.	Алгоритмы электронно-цифровой подписи. Особенности использования
5.	Технологии аутентификации.	Настройка политик, отвечающих за информационную безопасность
6.	Атаки на сервера и рабочие станции.	Сетевые защищенные протоколы. Защита от удаленных атак через сеть Internet.
7.	Технологии межсетевых экранов.	Особенности использования межсетевых экранов для обеспечения информационной безопасности
8.	Антивирусная защита.	Вопросы обновления антивирусных баз данных.
9.	Технологии построения защищенных информационных систем.	Способы и средства восстановления работоспособности.

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.	Основные понятия и определения информационной безопасности.	Опрос, тестирование.
2.	Понятие угрозы. Виды угроз информационной безопасности	Опрос, творческий проект, тестирование.
3.	Понятия утечки информации.	Опрос, информационный проект, тестирование.
4.	Криптографические методы защиты.	Опрос, творческий проект.
5.	Технологии аутентификации.	Опрос, тестирование.
6.	Атаки на сервера и рабочие станции.	Опрос, творческий проект, тестирование.
7.	Технологии межсетевых экранов.	Опрос, тестирование.
8.	Антивирусная защита.	Опрос, информационный проект, тестирование.

9.	Технологии построения защищенных информационных систем.	Опрос, тестирование.

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

8.1. Основная учебная литература:

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере: учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/89453.html

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

8.2. Дополнительная учебная литература:

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

2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. — Саратов: Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/72345.html

3. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/86938.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. Информационные технологии моделирования и управления. ISSN 1813-9744. https://www.iprbookshop.ru/43350.html .

3. Журнал «Образование и Информатика». http://infojournal.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

Система информационной безопасности предприятия

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.** Типовое проектирование информационных систем, а также различных моделей информационных систем и проектных спецификаций; Программные прототипы решения прикладных задач. **ПК-5.2.** Разработка ИС с учетом требований заказчика, на основе стандартов к проектированию информационных систем. Модификация существующих ИС для улучшения их функциональности и производительности. **ПК-5.3.** Способность разрабатывать мобильные приложения и работать с Интернет вещами **ПК-5.4.** Знать и уметь работать с технологиями искусственного интеллекта и инструментальными средствами разработки интеллектуальных программных систем. **ПК-5.5.** Верификация структуры программного кода ИС относительно архитектуры ИС. **ПК-5.6.** Создание пользовательские интерфейсы с учетом UX/UI принципов для повышения удобства использования ИС. **ПК-5.7.** Осуществляет поиск, анализ, программную реализацию математических моделей и алгоритмов интеллектуальной обработки данных.
ПК-6	Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.	**ПК-6.1.** Способен управлять процессом создания и модификации информационной системы, включая планирование, контроль выполнения работ, оценку и регулирование рисков. **ПК-6.2.** Владеет современными методами и средствами проектирования и разработки баз данных. **ПК-6.3.** Выполняет установку и настройку специализированных программных средств обеспечения безопасности, настройку параметров безопасности операционных систем сетевых устройств.

		ПК-6.4. Осуществляет поддержку и обслуживание ИС, в том числе решение проблемных ситуаций и устранение ошибок. **ПК-6.5.** Владеет инструментами для управления элементами ИТ-инфраструктуры при внедрении, эксплуатации и сопровождении информационных систем и сервисов. **ПК-6.6.** Интеграция различных компонентов ИС для обеспечения их эффективной работы. **ПК-6.7.** Понимает основы продуктовой разработки, может определить требования к продукту, планировать и управлять его разработкой, а также анализировать и учитывать потребности заказчика и конечных пользователей для достижения высокого уровня удовлетворения от использования продукта.

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. Основные стандарты и нормативы, касающиеся разработки и оформления технической документации в области информационных технологий. 2. Требования к технической документации, предъявляемые к профессионалам в области администрирования информационных систем и проектов. 3. Методы и подходы к структурированию и организации технической документации.	1.Умение составлять техническую документацию (технические задания, инструкции, руководства, отчеты) согласно установленным стандартам. 2. Навык работать с текстовыми и графическими редакторами для подготовки и оформления технической документации. 3. Умение структурировать информацию, делать ее легкодоступной и понятной для целевой аудитории. 4. Навык проведения	Навыками работы с документационными системами и инструментами для разработки технической документации (например, MS Word, Visio, Confluence). 2. Опытом использования шаблонов и стандартов оформления технической документации. 3. Навыками для эффективного взаимодействия с другими участниками проекта по вопросам разработки

	4. Принципы создания пользовательских инструкций и технических руководств. 5. Требования по защите конфиденциальности и безопасности информации в документации. 6. Принципы и методы контроля версий и изменений в технической документации.	анализа и интерпретации требований к технической документации. 5. Умение использовать терминологию и язык, соответствующие целевой аудитории документации. 6. Навык оформления диаграмм, схем и других графических элементов в технической документации.;	технической документации. 4. Умение работать в команде над разработкой согласованной технической документации. 5. Опыт управления временем и приоритетами при создании и обновлении документации. 6. Навык анализа и оценки качества технической документации для ее улучшения и совершенствования.
Код компетенции	**ПК-6**		
	- виды угроз информационных систем и методы обеспечения информационной безопасности; - основы информационной безопасности организации; - параметры безопасности и защиты программного обеспечения сетевых устройств, средства управления и обеспечения безопасности администрируемой сети.	- организовать комплексную защиту информационных систем; - определять параметры безопасности и защиты программного обеспечения сетевых устройств, устанавливать и администрировать средства управления и обеспечения безопасности администрируемой сети; - выполнять контроль использования ресурсов сетевых устройств и программного обеспечения; - оценивать производительность сетевой инфраструктуры инфокоммуникационн	- навыками выполнения регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы, восстановления параметров программного обеспечения сетевых устройств; - средствами контроля использование ресурсов сетевых устройств и программного обеспечения; - методами настройки сетевых элементов инфокоммуникационной системы; - правовыми, административными, программно-

		ой системы и использовать инструменты диагностики отказов и ошибок сетевых устройств.	аппаратными средствами информационной защиты, навыками работы с инструментальными средствами защиты информации.

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”.

При ответе на вопросы в рамках прохождения промежуточной аттестации (зачет/ зачет с оценкой/ экзамен) допускается вольная формулировка ответа, по смыслу раскрывающая содержание ответа, указанного в фонде оценочных средств, в качестве верного ответа.

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

4. Типовые контрольные задания (закрытого, открытого и иного типа) для проведения промежуточной аттестации, необходимые для оценки достижения

компетенции, соотнесенной с результатами обучения по дисциплине

ПК-5
7 СЕМЕСТР

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
a) Разработка аппаратных средств обеспечения правовых данных
b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
Ответ: c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
a) Хищение жестких дисков, подключение к сети, инсайдерство
b) Перехват данных, хищение данных, изменение архитектуры системы
c) Хищение данных, подкуп системных администраторов, нарушение регламента работы
Ответ: b) Перехват данных, хищение данных, изменение архитектуры системы

3. Виды информационной безопасности:
a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная
Ответ: a) Персональная, корпоративная, государственная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
a) несанкционированного доступа, воздействия в сети
b) инсайдерства в организации
c) чрезвычайных ситуаций
Ответ: a) несанкционированного доступа, воздействия в сети

5. Основные объекты информационной безопасности:
a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы
Ответ: a) Компьютерные сети, базы данных

6. Основными рисками информационной безопасности являются:
a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации
Ответ: c) Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:
a) Экономической эффективности системы безопасности
b) Многоплатформенной реализации системы
c) Усиления защищенности всех звеньев системы
Ответ: a) Экономической эффективности системы безопасности

8. Основными субъектами информационной безопасности являются:
a) руководители, менеджеры, администраторы компаний

b) органы права, государства, бизнеса
c) сетевые базы данных, фаерволлы
Ответ: b) органы права, государства, бизнеса

9. К основным функциям системы безопасности можно отнести все перечисленное:
a) Установление регламента, аудит системы, выявление рисков
b) Установка новых офисных приложений, смена хостинг-компании
c) Внедрение аутентификации, проверки контактных данных пользователей
Ответ: a) Установление регламента, аудит системы, выявление рисков

10. Принципом информационной безопасности является принцип недопущения:
a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности
Ответ: a) Неоправданных ограничений при работе в сети (системе)

11. Принципом политики информационной безопасности является принцип:
a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы
c) Полного блокирования доступа при риск-ситуациях
Ответ: a) Невозможности миновать защитные средства сети (системы)

12. Принципом политики информационной безопасности является принцип:
a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы
Ответ: Усиления защищенности самого незащищенного звена сети (системы)

Задания открытого типа

1. Какие существуют модели информационной безопасности?
2. Что такое коммерческая тайна?
3. Что относят к рискам информационной безопасности?

№ п/п	Вопрос	Ответ
1	Какие существуют модели информационной безопасности?	Модели информационной безопасности: Белла-ЛаПадулы (конфиденциальность), Биба (целостность), Кларка-Уилсона (правильность операций), Латтеса (уровни доступа), Абади-Збигнев (динамическое управление).
2	Что такое коммерческая тайна?	Коммерческая тайна — это информация, которая имеет ценность для бизнеса, не является общедоступной и защищена от разглашения в интересах организации.
3	Что относят к рискам информационной безопасности?	К рискам информационной безопасности относят угрозы утечек данных, несанкционированного доступа, хакерских атак, вирусных инфекций, потери или

		повреждения данных, а также ошибки пользователей и технические сбои.

ПК-6
7 СЕМЕСТР

1. Принципом политики информационной безопасности является принцип:
a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы
Ответ: a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

2. К основным типам средств воздействия на компьютерную сеть относится:
a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания
Ответ: b) Логические закладки («мины»)

3. Когда получен спам по e-mail с приложенным файлом, следует:
a) Прочитать приложение, если оно не содержит ничего ценного – удалить
b) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его
Ответ: c) Удалить письмо с приложением, не раскрывая (не читая) его

4. Принцип Кирхгофа:
a) Секретность ключа определена секретностью открытого сообщения
b) Секретность информации определена скоростью передачи данных
c) Секретность закрытого сообщения определяется секретностью ключа
Ответ: c) Секретность закрытого сообщения определяется секретностью ключа

5. ЭЦП – это:
a) Электронно-цифровой преобразователь
b) Электронно-цифровая подпись
c) Электронно-цифровой процессор
Ответ: b) Электронно-цифровая подпись

6. Наиболее распространены угрозы информационной безопасности корпоративной системы:
a) Покупка нелицензионного ПО
b) Ошибки эксплуатации и неумышленного изменения режима работы системы
c) Сознательного внедрения сетевых вирусов
Ответ: b) Ошибки эксплуатации и неумышленного изменения режима работы системы

7. Наиболее распространены угрозы информационной безопасности сети:
a) Распределенный доступ клиент, отказ оборудования
b) Моральный износ сети, инсайдерство
c) Сбой (отказ) оборудования, нелегальное копирование данных
Ответ: c) Сбой (отказ) оборудования, нелегальное копирование данных

8. Наиболее распространены средства воздействия на сеть офиса:
a) Слабый трафик, информационный обман, вирусы в интернет
b) Вирусы в сети, логические мины (закладки), информационный перехват
c) Компьютерные сбои, изменение администрирования, топологии
Ответ: b) Вирусы в сети, логические мины (закладки), информационный перехват

9. Утечкой информации в системе называется ситуация, характеризуемая:
a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации
Ответ: a) Потерей данных в системе

10. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
a) Целостность
b) Доступность
c) Актуальность
Ответ: a) Целостность

11. Угроза информационной системе (компьютерной сети) – это:
a) Вероятное событие
b) Детерминированное (всегда определенное) событие
c) Событие, происходящее периодически
Ответ: a) Вероятное событие

12. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
a) Регламентированной
b) Правовой
c) Защищаемой
Ответ: c) Защищаемой

13) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
a) Программные, технические, организационные, технологические
b) Серверные, клиентские, спутниковые, наземные
c) Личные, корпоративные, социальные, национальные
Ответ: a) Программные, технические, организационные, технологические

Задания открытого типа

1. Что такое технические каналы утечки информации?
2. Что такое эвристический алгоритм поиска вирусов?
3. Что такое криптография?

№ п/п	Вопрос	Ответ
1	Что такое технические каналы утечки информации?	Технические каналы утечки информации — это пути, через которые может происходить несанкционированный вывод

		или передача конфиденциальных данных, например, через уязвимости в сети, устройствах хранения, беспроводных каналах или в процессах обработки информации.
2	Что такое эвристический алгоритм поиска вирусов?	Эвристический алгоритм поиска вирусов — это метод, использующий набор правил и анализ поведения файлов или программ для выявления вирусов, даже если их точные сигнатуры ещё не известны.
3	Что такое криптография?	Криптография — это наука о защите информации с помощью кодирования, шифрования и декодирования данных для обеспечения их конфиденциальности, целостности и подлинности.