

АВТНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ СОЦИАЛЬНЫЙ ИНСТИТУТ»



Утверждаю
Декан ФИСТ Ж.В. Игнатенко
«20» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) программы: Цифровизация экономической деятельности

Квалификация выпускника: Бакалавр

Форма обучения: очная, заочная

Год начала подготовки – 2024

Разработана
Канд. техн. наук, доцент
С.В. Аникуев

Согласована
зав. кафедрой ПИМ
Д.Г. Ловянников

Рекомендована
на заседании кафедры ИС
от «17» мая 2024 г.
протокол № 9
Зав. кафедрой А.Ю. Орлова

Одобрена
на заседании учебно-методической
комиссии ФИСТ
от «20» мая 2024 г.
протокол № 9
Председатель УМК Ж.В. Игнатенко

Ставрополь, 2024 г.

Содержание

1. Цели освоения дисциплины	3
1. Понимать сущность информационной безопасности.....	3
2. Понимать принципы организации защиты информации на предприятиях.	3
3. Выявлять основные виды угроз информационной безопасности.	3
4. Применять программно-аппаратные средства для обеспечения информационной безопасности.	3
2. Место дисциплины в структуре опоп	3
3. Планируемые результаты обучения по дисциплине	3
4. Объем дисциплины и виды учебной работы	5
5. Содержание и структура дисциплины.....	6
5.1. Содержание дисциплины	6
5.2. Структура дисциплины.....	8
5.3. Занятия семинарского типа	10
5.4. Курсовой проект (курсовая работа, реферат, контрольная работа)	11
5.5. Самостоятельная работа	12
6. Образовательные технологии.....	13
7. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации	13
8. Учебно-методическое и информационное обеспечение дисциплины	24
8.1. Основная литература	24
8.3. Программное обеспечение	24
8.4. Профессиональные базы данных.....	25
8.5. Информационные справочные системы	25
8.6. Интернет-ресурсы	25
8.7. Методические указания по освоению дисциплины.....	25
9. Материально-техническое обеспечение дисциплины	30
10. Особенности освоения дисциплины лицами с ограниченными возможностями здоровья	30

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность» является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи при изучении дисциплины:

1. Понимать сущность информационной безопасности.
2. Понимать принципы организации защиты информации на предприятиях.
3. Выявлять основные виды угроз информационной безопасности.
4. Применять программно-аппаратные средства для обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» входит в обязательную часть Блока 1 ОПОП.

Предшествующие дисциплины (курсы, модули, практики)	Последующие дисциплины (курсы, модули, практики)
Информатика и программирование Операционные системы Информационные системы и технологии	Архитектуры информационных систем Вычислительные системы сети и телекоммуникации Методы и средства проектирования информационных систем и технологий Администрирование информационных систем Базы данных Корпоративные информационные системы и сети Интернет-программирование Методы и средства защиты информации организации

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 3.1. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

	<p>ОПК 3.2. Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.</p>	<p>Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>
--	---	---

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общий объем дисциплины составляет 5 зачетных единицы, 180 академических часа.

Очная форма обучения

Вид учебной работы	Всего часов	Триместры
		8
Контактная работа (всего)	40	40
в том числе:		
1) занятия лекционного типа (ЛК)	20	20
из них		
– лекции	20	20
2) занятия семинарского типа (ПЗ)		
из них		
– семинары (С)		
– практические занятия (ПР)	30	30
– лабораторные работы (ЛР)		
3) групповые консультации		
4) индивидуальная работа		
5) промежуточная аттестация		
Самостоятельная работа (всего) (СР)	130	130
в том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Контрольная работа		
Реферат	30	30
Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумами т.д.)	100	140
Подготовка к аттестации		
Общий объем, час	180	180
Форма промежуточной аттестации(дифференцированный зачет)	Диф. зачет	Диф. зачет

Заочная форма обучения

Вид учебной работы	Всего часов	Триместры
		8
Контактная работа (всего)	8,3	8,3
в том числе:		
1) занятия лекционного типа (ЛК)	4	4
из них		
– лекции	4	4
2) занятия семинарского типа (ПЗ)	4	4
из них		
– семинары (С)		
– практические занятия (ПР)	4	4
– лабораторные работы (ЛР)		

3) групповые консультации		
4) индивидуальная работа		
5) промежуточная аттестация	0,3	0,3
Самостоятельная работа (всего) (СР)	168	168
в том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Контрольная работа		
Реферат	20	20
Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумами т.д.)	112	112
Подготовка к аттестации	3,7	3,7
Общий объем, час	180	180
Форма промежуточной аттестации(дифференцированный зачет)	Диф. зачет	Диф. зачет

5. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

5.1. Содержание дисциплины

№ раздела (темы)	Наименование раздела (темы)	Содержание раздела (темы)
1 раздел. Основопологающие положения		
1.1	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.	Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность.
1.2	Виды противников или «нарушителей». Понятие о видах вирусов.	Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.
1.3	Три вида возможных нарушений информационной системы. Защита.	Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.
1.4	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.

2 раздел. Основные положения теории информационной безопасности		
2.1	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.
2.2	Основные положения теории информационной безопасности. Модели безопасности и их применение.	Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности.
2.3	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы.
2.4	Анализ способов нарушений информационной безопасности.	Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
3 раздел. Защита информации		
3.1	Использование защищенных компьютерных систем.	Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.
3.2	Основные положения теории информационной безопасности. Модели безопасности и их применение.	Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике.
3.3	Методы криптографии	Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Виженера. Программы для криптографии. Электронная цифровая подпись.
3.4	Основные технологии построения защищенных систем.	Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности

		использования средств информационной защиты.
3.5	Место информационной безопасности экономических систем в национальной безопасности страны	Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.

5.2. Структура дисциплины

Очная форма обучения

№ раздела (темы)	Наименование раздела (темы)	Количество часов					
		Всего	ЛК	С	ПР	ЛР	СР
1 раздел. Основополагающие положения							
1.1	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.	11	1		2		8
1.2	Виды противников или «нарушителей». Понятие о видах вирусов.	11	1		2		8
1.3	Три вида возможных нарушений информационной системы. Защита.	7	1				6
1.4	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	11	1		2		8
	Общий объем 1 раздела	40	4		6		30
2 раздел. Основные положения теории информационной безопасности							
2.1	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	11	2		1		8
2.2	Основные положения теории информационной безопасности. Модели безопасности и их применение.	11	2		1		8
2.3	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	12	4				8
2.4	Анализ способов нарушений информационной безопасности.	12	4				8

	Общий объем 2 раздела	46	12		2		32
3 раздел. Защита информации							
3.1	Использование защищенных компьютерных систем.	11	1		2		8
3.2	Основные положения теории информационной безопасности. Модели безопасности и их применение.	11	1		2		8
3.3	Методы криптографии	13	1		2		10
3.4	Основные технологии построения защищенных систем.	11	1		2		8
3.5	Место информационной безопасности экономических систем в национальной безопасности страны	12			4		8
Общий объем 3 раздела		58	4		12		42
Групповая консультация							
Промежуточная аттестация							
Общий объем		180	20		20		104

Заочная форма обучения

№ раздела (темы)	Наименование раздела (темы)	Количество часов					
		Всего	ЛК	С	ПР	ЛР	СР
1 раздел. Основопологающие положения							
1.1	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.	12	1		1		10
1.2	Виды противников или «нарушителей». Понятие о видах вирусов.	12	1		1		10
1.3	Три вида возможных нарушений информационной системы. Защита.	11			1		10
1.4	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	11			1		10
Общий объем 1 раздела		46	2		4		40
2 раздел. Основные положения теории информационной безопасности							
2.1	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	11	1				10
2.2	Основные положения теории информационной безопасности.	11	1				10

	Модели безопасности и их применение.					
2.3	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	10				10
2.4	Анализ способов нарушений информационной безопасности.	10				10
	Общий объем 2 раздела	42	2			40
3 раздел. Защита информации						
3.1	Использование защищенных компьютерных систем.	10				10
3.2	Основные положения теории информационной безопасности. Модели безопасности и их применение.	10				10
3.3	Методы криптографии	10				10
3.4	Основные технологии построения защищенных систем.	10				10
3.5	Место информационной безопасности экономических систем в национальной безопасности страны	12				12
	Общий объем 3 раздела	52				52
	Групповая консультация					
	Промежуточная аттестация	4		4		
	Общий объем	180	4	4	4	132

5.3. Занятия семинарского типа

Очная форма обучения

№ п/п	№ раздела (темы)	Вид занятия	Наименование	Количество часов
1	1.1	ПЗ	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.	2
2	1.2	ПЗ	Виды противников или «нарушителей». Понятие о видах вирусов.	2
3	1.4	ПЗ	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	2
4	2.1, 2.2	ПЗ	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	2
5	3.1	ПЗ	Использование защищенных компьютерных систем.	2
6	3.2	ПЗ	Основные положения теории	2

			информационной безопасности. Модели безопасности и их применение.	
7	3.3	ПЗ	Методы криптографии	2
8	3.4	ПЗ	Основные технологии построения защищенных систем.	2
9	3.5	ПЗ	Место информационной безопасности экономических систем в национальной безопасности страны	4

Заочная форма обучения

№ п/п	№ раздела (темы)	Вид занятия	Наименование	Количество часов
1	1.1, 1.2	ПЗ	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятие о видах вирусов.	2
2	1.3, 1.4	ПЗ	Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	2

5.4. Курсовой проект (курсовая работа, реферат, контрольная работа)

Примерные темы рефератов:

- 1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
- 2 Современные средства защиты информации
- 3 Современные системы компьютерной безопасности
- 4 Современные средства противодействия экономическому шпионажу
- 5 Современные криптографические системы
- 6 Криптоанализ, современное состояние
- 7 Правовые основы защиты информации
- 8 Технические аспекты обеспечения защиты информации. Современное состояние
- 9 Атаки на систему безопасности и современные методы защиты
- 10 Современные пути решения проблемы информационной безопасности РФ
- 11 Общая проблема информационной безопасности информационных систем. Основные понятия информационной безопасности. Санкционированный и несанкционированный доступ.
- 12 Общая проблема информационной безопасности информационных систем. Базовые свойства информационной безопасности. Угрозы безопасности и каналы реализации угроз.
- 13 Общая проблема информационной безопасности информационных систем. Основные принципы разграничения информационной безопасности. Ценность информации.
- 14 Общая проблема информационной безопасности информационных систем. Меры обеспечения безопасности компьютерных систем.

- 15 Защита информации при реализации информационных процессов.
- 16 Защита информации при реализации информационных процессов.
- 17 Идентификация и аутентификация субъектов
- 18 Организационное обеспечение информационной безопасности. Классификация политик безопасности
- 19 Организационное обеспечение информационной безопасности. Модели контроля целостности
- 20 Организационное обеспечение информационной безопасности. Модели контроля безопасности
- 21 Защита информации от несанкционированного доступа
- 22 Математические и методические средства защиты. Элементы теории чисел
- 23 Математические и методические средства защиты. Принципы криптографической защиты.
- 24 Математические и методические средства защиты. Симметричные криптосистемы.
- 25 Математические и методические средства защиты. Ассиметричные криптосистемы.
- 26 Математические и методические средства защиты. Стандарты шифрования различных стран.
- 27 Компьютерные средства реализации защиты в информационных системах. Контроль целостности информации.
- 28 Компьютерные средства реализации защиты в информационных системах. Электронно-цифровая подпись
- 29 Компьютерные средства реализации защиты в информационных системах. Хранение и распределение ключевой информации.
- 30 Компьютерные средства реализации защиты в информационных системах. Протоколы безопасной аутентификации пользователей
- 31 Компьютерные средства реализации защиты в информационных системах. Защита от разрушающих программных воздействий
- 32 Компьютерные средства реализации защиты в информационных системах. Защита информации в компьютерных сетях
- 33 Программа информационной безопасности России и пути ее реализации. Руководящие документы России
- 34 Программа информационной безопасности России и пути ее реализации. Инженерно-техническая защита информации
- 35 Программа информационной безопасности России и пути ее реализации. Правовое обеспечение информационной безопасности

На первой неделе триместра производится выдача тем рефератов, защита рефератов производится на последней неделе триместра.

5.5. Самостоятельная работа

Очная форма обучения

№ раздела (темы)	Виды самостоятельной работы	Количество часов
1-3	Проработка и повторение лекционного материала	40
1-3	Подготовка к практическим занятиям	44
1-3	Реферат	20
1-3	Подготовка к аттестации	

Заочная форма обучения

№ раздела (темы)	Виды самостоятельной работы	Количество часов
1-3	Проработка и повторение лекционного материала	52
1-3	Подготовка к практическим занятиям	60
1-3	Реферат	20
1-3	Подготовка к аттестации	3,7

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

При чтении лекций используется компьютерная техника для демонстрации слайдов с помощью программного приложения MicrosoftPowerPoint. На практических занятиях студенты представляют результаты выполнения самостоятельной работы, подготовленные с помощью программного приложения MicrosoftOffice. При выполнении практических заданий студентами используется программное обеспечение: ОСWindows иMSOffice.

Интерактивные и активные образовательные технологии

№ раздела (темы)	Вид занятия (ЛК, ПР, С, ЛР)	Используемые интерактивные и активные образовательные технологии	Количество часов ОФО/ЗФО
1.2	Л	Виртуальная экскурсия «Виды противников или «нарушителей». Понятие о видах вирусов».	1/1
3.3	Л	Виртуальная экскурсия «Методы криптографии».	1/0
2.1	Л	Дискуссия.	2/1
3.5	ПР	Опережающая самостоятельная работа студентов.	1/0

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Описание показателей оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Таблица 1 – Показатели оценивания и оценочные средства для оценивания результатов обучения по дисциплине

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Показатели оценивания (результаты обучения)	Процедуры оценивания (оценочные средства)	
			текущий контроль успеваемости	промежуточная аттестация

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Показатели оценивания (результаты обучения)	Процедуры оценивания (оценочные средства)	
			текущий контроль успеваемости	промежуточная аттестация
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 3.1. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.	Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования	Контрольные вопросы Тестовое задание	Диф.зачет (контрольные вопросы, тестовое задание)
	ОПК 3.2. Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Практическое задание	Диф. зачет (ситуационная задача)
		Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Практическое задание	Диф. зачет (ситуационная задача)

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Показатели оценивания (результаты обучения)	Процедуры оценивания (оценочные средства)	
			текущий контроль успеваемости	промежуточная аттестация
ОПК-3				Диф.зачет

ОЦЕНОЧНЫЕ СРЕДСТВА, КРИТЕРИИ И ШКАЛА ОЦЕНКИ

Типовые задания для текущего контроля.

Перечень типовых контрольных вопросов для устного опроса

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.
5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).
14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус.
18. Понятия и пути распространения вирусов. Основные способы заражения программ.
19. Основные общие нормативные правовые акты.
20. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
21. Руководящие документы и методические указания в сфере защиты информации.
22. Персональные данные, их классификация.
23. Правовые основы использования персональных данных.
24. Принципы обработки персональных данных.
25. Создание и оценка соответствия информационной системы персональных данных.
26. Права субъектов персональных данных.
27. Обязанности оператора при обработке персональных данных.
28. Электронная цифровая подпись.

Типовые ситуационные задачи

Практическая задача №1

Вы – сотрудник лечебного учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.
2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Практическая задача №2

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?
2. Какие символы должны быть использованы при записи пароля?

Практическая задача №3

Гражданин П. проник в информационную базу ККБ и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

1. Являются ли его действия противозаконными?
2. С чем это связано?
3. Какое наказание может ждать гражданина П. за совершенные им действия?

Практическая задача №4

Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Практическая задача №5

Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Типовые тестовые задания

1. Под информационной безопасностью понимается...
 - А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
 - Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
 - В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

1. Доступность – это...

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

2. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

3. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

4. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

5. Целостность можно подразделить:

А) статическую

Б) динамическую

В) структурную

Типовые задания для промежуточной аттестации

Контрольные вопросы для промежуточной аттестации (экзамен)

1. История возникновения проблемы защиты информации.

2. Причины утечки и искажения информации.

3. Требования, предъявляемые к уровню обеспечения информационной безопасности (ИБ).

4. Надёжность и уязвимость информации в информационных системах.

5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).
14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус. Понятия и пути распространения вирусов.
18. Основные способы заражения программ.
19. Основные классы вирусов.
20. Классификация закладок и их общие характеристики.
21. Саморазмножающиеся и другие разновидности закладок.
22. Троянский конь. Структура и способы распространения.
23. Временная и логическая бомба. Структура и способы распространения.
24. Винлокер. Структура и способы распространения.
25. Червь. Структура и способы распространения.
26. Признаки проявления вредоносных программ.
27. Классификация угроз для мобильных устройств.
28. Характеристика вредоносных программы для мобильных устройств.
29. Программы-вымогатели для мобильных устройств.
30. Методики оценки рисков в сфере информационной безопасности.
31. Своевременная компьютерная профилактика от вирусов.
32. Использование антивирусной защиты.
33. Классификация антивирусных программ.
34. Основы безопасности мобильных устройств.
35. Методы защиты мобильных устройств от киберугроз.
36. Программное обеспечение для оценки рисков информационной безопасности.
37. Содержание и структура правового обеспечения информационной безопасности.
38. Государственное регулирование отношений в сфере защиты информации.
39. Основные нормативно-правовые акты и методические документы в области защиты информации.
40. Основные общие нормативные правовые акты по вопросам информационной безопасности.
41. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
42. Персональные данных, их классификация.
43. Принципы обработки персональных данных.
44. Создание и оценка соответствия информационной системы персональных данных.
45. Права субъектов персональных данных.
46. Обязанности оператора при обработке персональных данных.
47. Электронная цифровая подпись.

Типовые задания для промежуточного контроля

Перечень типовых контрольных вопросов для устного опроса на промежуточной аттестации (дифференцированного зачета)

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?

40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейного криптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL -списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?
66. Из чего состоит высоконадежная вычислительная база (ТСВ)?
67. Какие модели многоуровневой защиты вы знаете?
68. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70. Какие задачи решает система компьютерной безопасности?
71. Какие пути защиты информации в локальной сети существуют?
72. Какие задачи решают технические средства противодействия экономическому шпионажу?
73. Какой порядок организации системы видеонаблюдения?
74. Что включает в себя защита информационных систем с помощью планирования?
75. Какие условия работы оцениваются при планировании?
76. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77. Что такое мобильные программы?
78. Что такое концепция потоков?
79. Что представляет собой метод «песочниц»?
80. Что такое интерпретация?
81. Что такое программы с подписями?
82. Что представляет собой безопасность в системе Java ?

83. Назовите несколько примеров политик безопасности пакета JDK 1.2?
84. Какими международными документами регламентируется деятельность по обеспечению защиты информации?
85. Что понимают под политикой информационной безопасности?
86. Что включает в себя политика информационной безопасности РФ?
87. Какие нормативные документы РФ определяют концепцию защиты информации?

Критерии и шкала оценки дифференцированного зачета по дисциплине

Оценка	Характеристики ответа обучающегося
Отлично	<ul style="list-style-type: none"> - студент глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой понятий по дисциплине; - правильно решил ситуационную задачу.
Хорошо	<ul style="list-style-type: none"> - студент твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой понятий по дисциплине; - правильно решил ситуационную задачу.
Удовлетворительно	<ul style="list-style-type: none"> - студент усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой понятий по дисциплине; - с затруднениями решил ситуационную задачу.
Неудовлетворительно	<ul style="list-style-type: none"> - студент не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений; - не решил ситуационную задачу

Методические материалы, определяющие процедуры оценивания

Методические материалы, определяющие процедуры оценивания в рамках текущего контроля успеваемости

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося.

Краткая характеристика процедуры реализации текущего и промежуточного контроля для оценки компетенций обучающихся представлена в таблице.

Процедура оценивания	Организация деятельности обучающегося
Практическое задание	Оценочное средство, включающее совокупность условий, направленных на выполнение практического задания с целью формирования компетенций, соответствующих основным типам профессиональной деятельности. Процедура проведения данного оценочного мероприятия включает в себя: оценку правильности выполнения практического задания
Устный опрос	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях. Показатели для оценки устного ответа: 1) знание материала; 2) последовательность изложения; 3) владение речью и профессиональной терминологией; 4) применение конкретных примеров; 5) знание ранее изученного материала; 6) уровень теоретического анализа; 7) степень самостоятельности; 8) степень активности в процессе; 9) выполнение регламента. Уровень знаний обучающегося определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Критерии и шкала оценки приведены в п. 3. Фонда оценочных средств.
Выполнение тестовых заданий	Это средство контроля полноты усвоения понятий, представлений, существенных

	<p>положений отдельных тем (разделов) дисциплины.</p> <p>Процедура проведения данного оценочного мероприятия включает в себя: осуществляется по вариантам; количество вопросов в каждом варианте –10-15; отведенное время– 90 мин. Решение заданий в тестовой форме проводится в течение изучения дисциплины.</p> <p>Для подготовки к данному оценочному мероприятию студенты должны изучить разделы (темы, вопросы), по которым будут задания в тестовой форме, и теоретические источники для подготовки.</p> <p>При проведении тестирования, студенту запрещается пользоваться дополнительной литературой.</p>
--	--

Методические материалы, определяющие процедуры оценивания в рамках промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета.

Дифференцированный зачет – это форма промежуточной аттестации по дисциплине, задачей которой является комплексная оценка уровней достижения планируемых результатов обучения по дисциплине.

Дифференцированный зачет по дисциплине включает в себя: ответ на контрольный вопрос, тестовое задание и одну ситуационную задачу.

Контрольный вопрос	<p>Контрольный вопрос — это средство контроля усвоения учебного материала дисциплины.</p> <p>Процедура проведения данного оценочного мероприятия включает в себя: беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме дисциплины.</p>
Тестовое задание	<p>Оценочное средство, варьирующееся по элементам содержания и по трудности, единица контрольного материала, сформулированная в утвердительной форме предложения с неизвестным. Подстановка правильного ответа вместо неизвестного компонента превращает задание в истинное высказывание, подстановка неправильного ответа приводит к образованию ложного высказывания, что свидетельствует о незнании студентом данного учебного материала.</p>

Ситуационная задача	Оценочное средство, включающее совокупность условий, направленных на решение практически значимой ситуации с целью формирования компетенций, соответствующих основным типам профессиональной деятельности. Процедура проведения данного оценочного мероприятия включает в себя: оценку правильности решения задач, разбор результатов. В случае вариативности решения задачи следует обосновать все возможные варианты решения.
---------------------	--

После окончания ответа преподаватель объявляет обучающемуся оценку по результатам зачета, а также вносит эту оценку в зачетно-экзаменационную ведомость, зачетную книжку.

Уровень знаний, умений и навыков обучающегося определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература

Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <http://www.iprbookshop.ru/80290.html>

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 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <http://www.iprbookshop.ru/87995.html>

8.2. Дополнительная литература

Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <http://www.iprbookshop.ru/86357.html>

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 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <http://www.iprbookshop.ru/72345.html>

Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Д. В. Фомин. — Саратов : Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/110329.html>



8.3. Программное обеспечение

Microsoft Windows, Яндекс 360, Microsoft Office Professional Plus 2019, Google Chrome, Яндекс.Браузер.

8.4. Профессиональные базы данных

1. Национальный открытый университет Интуит – интернет университет информационных технологий <http://www.intuit.ru/>
2. Справочно-правовая система «КонсультантПлюс» <http://www.consultant.ru/>

8.5. Информационные справочные системы

Справочно-правовая система «КонсультантПлюс» - <http://www.consultant.ru/>
Поисковые системы
Поисковая система Yandex- <https://www.yandex.ru/>
Поисковая система Rambler – <https://www.rambler.ru/>

8.6. Интернет-ресурсы

- 1 Цифровой образовательный ресурс IPR SMART-<http://www.iprbookshop.ru/>
- 2 ООО «Электронное издательство Юрайт». Образовательная платформа Юрайт - <https://urait.ru/>
- 3 Национальный открытый университет Интуит – интернет университет информационных технологий <http://www.intuit.ru/>

8.7. Методические указания по освоению дисциплины

Методические рекомендации при работе над конспектом во время проведения лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Общие и утвердившиеся в практике правила и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их.

В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

Методические рекомендации по подготовке к практическим(семинарским) работам

Целью практических(семинарских) работ является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическим работам необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы. Желательно при подготовке к практическим и лабораторным работам по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа приводит обучающегося к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений.

Самостоятельная работа выполняет ряд функций:

- развивающую;
- информационно-обучающую;
- ориентирующую и стимулирующую;
- воспитывающую;
- исследовательскую.

Виды самостоятельной работы, выполняемые в рамках курса:

1. Проработка и повторение лекционного материала
2. Подготовка к практическим занятиям
3. Реферат
4. Подготовка к аттестации

Обучающимся рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые обучающийся получает в аудитории.

Можно отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала.

Методические рекомендации по написанию реферата

Написание реферата является

- одной из форм обучения студентов, направленной на организацию и повышение уровня самостоятельной работы студентов;
- одной из форм научной работы студентов, целью которой является расширение научного кругозора студентов, ознакомление с методологией научного поиска.

Реферат, как форма обучения студентов, - это краткий обзор максимального количества доступных публикаций по заданной теме, с элементами сопоставительного анализа данных материалов и с последующими выводами.

При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируются уже сделанные предыдущими исследователями выводы и в связи с небольшим объемом данной формы работы.

Темы рефератов определяются кафедрой и содержатся в программе курса. Преподаватель рекомендует литературу, которая может быть использована для написания реферата.

Целью написания рефератов является:

- привитие студентам навыков библиографического поиска необходимой литературы (на бумажных носителях, в электронном виде);
- привитие студентам навыков компактного изложения мнения авторов и своего суждения по выбранному вопросу в письменной форме, научно грамотным языком и в хорошем стиле;
- приобретение навыка грамотного оформления ссылок на используемые источники, правильного цитирования авторского текста;
- выявление и развитие у студента интереса к определенной научной и практической проблематике с тем, чтобы исследование ее в дальнейшем продолжалось в подготовке и написании курсовых и дипломной работы и дальнейших научных трудах.

Основные задачи студента при написании реферата:

- с максимальной полнотой использовать литературу по выбранной теме (как рекомендуемую, так и самостоятельно подобранную) для правильного понимания авторской позиции;
- верно (без искажения смысла) передать авторскую позицию в своей работе;
- уяснить для себя и изложить причины своего согласия (несогласия) с тем или иным автором по данной проблеме.

Требования к содержанию:

- материал, использованный в реферате, должен относиться строго к выбранной теме;
- необходимо изложить основные аспекты проблемы не только грамотно, но и в соответствии с той или иной логикой (хронологической, тематической, событийной и др.);
- при изложении следует сгруппировать идеи разных авторов по общности точек зрения или по научным школам;
- реферат должен заканчиваться подведением итогов проведенной исследовательской работы: содержать краткий анализ-обоснование преимуществ той точки зрения по рассматриваемому вопросу, с которой Вы солидарны.

Структура реферата.

1. Начинается реферат с *титulyного листа*.

Образец оформления титульного листа для реферата находится на сайте sksi.ru

2. За титульным листом следует *Содержание*. Содержание - это план реферата, в котором каждому разделу должен соответствовать номер страницы, на которой он находится.

3. *Текст* реферата. Он делится на три части: *введение, основная часть и заключение*.

а) *Введение* – раздел реферата, посвященный постановке проблемы, которая будет рассматриваться и обоснованию выбора темы.

б) *Основная часть* – это звено работы, в котором последовательно раскрывается выбранная тема. Основная часть может быть представлена как цельным текстом, так и разделена на главы. При необходимости текст реферата может дополняться иллюстрациями, таблицами, графиками, но ими не следует "перегружать" текст.

в) *Заключение* – данный раздел реферата должен быть представлен в виде выводов, которые готовятся на основе подготовленного текста. Выводы должны быть краткими и четкими. Также в заключении можно обозначить проблемы, которые "высветились" в ходе работы над рефератом, но не были раскрыты в работе.

4. *Список источников и литературы*. В данном списке называются как те источники, на которые ссылается студент при подготовке реферата, так и все иные, изученные им в связи с его подготовкой. В работе должно быть использовано не менее 5 разных источников. Работа, выполненная с использованием материала, содержащегося в одном научном источнике, является явным плагиатом и не принимается. Оформление Списка источников и литературы должно соответствовать требованиям

библиографических стандартов (например, Воробьева Ф.И. Информатика. MS Excel 2010 [Электронный ресурс]: учебное пособие/ Воробьева Ф.И., Воробьев Е.С. – Электрон.текстовые данные. – Казань: Казанский национальный исследовательский технологический университет, 2014. – 100 с. – Режим доступа: <http://www.iprbookshop.ru/62175.html>. – ЭБС «IPRbooks»).

Объем работы должен быть, как правило, не менее 12 и не более 20 страниц. Работа должна выполняться через одинарный интервал 12 шрифтом, размеры оставляемых полей: левое – 25 мм, правое – 15 мм, нижнее – 20 мм, верхнее – 20 мм. Страницы должны быть пронумерованы.

Расстояние между названием части реферата или главы и последующим текстом должно быть равно трем интервалам. Фразы, начинающиеся с "красной" строки, печатаются с абзацным отступом от начала строки, равным 1 см.

При цитировании необходимо соблюдать следующие правила:

– текст цитаты заключается в кавычки и приводится без изменений, без произвольного сокращения цитируемого фрагмента (пропуск слов, предложений или абзацев допускается, если не влечет искажения всего фрагмента, и обозначается многоточием, которое ставится на месте пропуска) и без искажения смысла;

– каждая цитата должна сопровождаться ссылкой на источник, библиографическое описание которого должно приводиться в соответствии с требованиями библиографических стандартов.

Оценивая реферат, преподаватель обращает внимание на:

- соответствие содержания выбранной теме;
- отсутствие в тексте отступлений от темы;
- соблюдение структуры работы, четка ли она и обоснованна;
- умение работать с научной литературой – вычленять проблему из контекста;
- умение логически мыслить;
- культуру письменной речи;
- умение оформлять научный текст (правильное применение и оформление ссылок, составление библиографии);
- умение правильно понять позицию авторов, работы которых использовались при написании реферата;
- способность верно, без искажения передать используемый авторский материал;
- соблюдение объема работы;
- аккуратность и правильность оформления, а также технического выполнения работы.

Реферат должен быть сдан для проверки в установленный срок.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой следует учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность обучающемуся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к лабораторным практикумам по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в приведенном в ФОС перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью изучающего чтения является глубокое и всестороннее понимание учебной информации.

Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:

- медленно прочитать текст, стараясь понять смысл изложенного;
- выделить ключевые слова в тексте;
- постараться понять основные идеи, подтекст и общий замысел автора.

3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Методические указания по подготовке к промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета.

Дифференцированный зачет – это форма промежуточной аттестации, задачей которой является комплексная оценка уровней достижения планируемых результатов обучения по дисциплине.

Для допуска студенту необходимо выполнить и успешно сдать практические работы (практические задания) по каждой теме.

При подготовке к дифференцированному зачету необходимо повторить конспекты лекций по всем разделам дисциплины. На дифференцированном зачете студент должен подтвердить усвоение учебного материала, предусмотренного рабочей программой дисциплины, а также продемонстрировать приобретенные навыки адаптации полученных теоретических знаний к своей профессиональной деятельности. Дифференцированный зачет проводится в форме устного собеседования по контрольным вопросам, а также обучающемуся необходимо решить ситуационную задачу.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины требуется следующее материально-техническое обеспечение (специальные помещения):

- для проведения занятий лекционного типа
учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.
- для проведения занятий семинарского типа, практических занятий
учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.
- для проведения, текущего контроля и промежуточной аттестации
учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.
- для групповых и индивидуальных консультаций
учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.
- для самостоятельной работы:
помещение, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Института.

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (тьютора), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
 - присутствие тьютора, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
 - письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
 - специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
 - индивидуальное равномерное освещение не менее 300 люкс,
 - при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

– присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются тьютору;

– по желанию студента задания могут выполняться в устной форме.
