

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ

Кафедра информационных технологий и систем

ТЕХНОЛОГИИ ПОСТРОЕНИЯ СИСТЕМ ОТОБРАЖЕНИЯ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

09.03.03 Прикладная информатика

Прикладная информатика в гуманитарной сфере

Уровень высшего образования: бакалавриат

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

ТЕХНОЛОГИИ ПОСТРОЕНИЯ СИСТЕМ ОТОБРАЖЕНИЯ ИНФОРМАЦИИ

Рабочая программа дисциплины

Составитель:

к.х.н., доцент А.М. Подорожный

.....

Ответственный редактор

к.с.-х.н., доц, и.о .зав.кафедрой Н.Ш. Шукенбаева

УТВЕРЖДЕНО

Протокол заседания кафедры ИТС

№ 10 от 04.04.2022г.

ОГЛАВЛЕНИЕ

1	Пояснительная записка	4
1.1	Цель и задачи дисциплины	4
1.2	Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций:	4
1.3	Место дисциплины в структуре образовательной программы.	5
2	Структура дисциплины	5
3	Содержание дисциплины «Технологии построения систем отображения информации».....	5
4	Образовательные технологии.....	7
5	Оценка планируемых результатов обучения	9
5.1	Система оценивания.....	9
5.2	Критерии выставления оценки по дисциплине	10
5.3	Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.	11
6	Учебно-методическое и информационное обеспечение дисциплины	20
6.1	Список источников и литературы.....	20
6.2	Перечень ресурсов информационно-телекоммуникационной сети «Интернет». .	21
6.3	Профессиональные базы данных и информационно-справочные системы	21
7	Материально-техническое обеспечение дисциплины.	21
8	Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья	21
9	Методические материалы	22
9.1	Планы практических занятий.....	22
	<i>Приложение 1</i>	24
	АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	24

1 Пояснительная записка

1.1 Цель и задачи дисциплины.

Цель дисциплины – познание средств отображения информации, представляющих собой сочетание программных и аппаратных средств обмена информацией между человеком и различными автоматизированными и вычислительными системами.

Задачи дисциплины: получение знаний по аппаратным и программным способам реализации средств отображения информации и приобретение навыков проектирования сложных систем на основе комплексного подхода, учитывающего психофизиологические особенности восприятия, методы формирования информационных моделей, фотометрических характеристик электронных индикаторов, структуры и режимы устройств управления ими.

1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-6 – Способен настраивать, эксплуатировать и сопровождать информационные системы и сервисы.	ПК-6.1 – Знает методы настройки, порядок и мероприятия по эксплуатации и сопровождению информационных систем и сервисов.	<i>Знать:</i> методы настройки, порядок и мероприятия по эксплуатации и сопровождению информационных систем и сервисов.
	ПК-6.2 – Умеет организовывать настройку, эксплуатацию и сопровождение информационных систем и сервисов.	<i>Уметь:</i> организовывать настройку, эксплуатацию и сопровождение информационных систем и сервисов.
	ПК – 6.3 – Владеет навыками управления конфигурацией ИС и сервисов в процессе эксплуатации, решения проблем и консультирования пользователей информационных систем и сервисов.	<i>Владеть:</i> навыками управления конфигурацией ИС и сервисов в процессе эксплуатации, решения проблем и консультирования пользователей информационных систем и сервисов.
ПК-8 – Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.	ПК-8.1 – Знает способы организации ИТ-инфраструктуры, методы и приемы управления информационной безопасностью.	<i>Знать:</i> способы организации ИТ-инфраструктуры, методы и приемы управления информационной безопасностью.
	ПК-8.2 – Умеет организовывать ИТ-инфраструктуру	<i>Уметь:</i> организовывать ИТ-инфраструктуру предприятия и процессы управления

	предприятия и процессы управления информационной безопасностью.	информационной безопасностью.
	<i>ПК-8.3</i> – Владеет навыками организации ИТ-инфраструктуры и управления информационной безопасностью.	<i>Владеть:</i> навыками организации ИТ-инфраструктуры и управления информационной безопасностью.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Технологии построения систем отображения информации» относится к вариативной части блока дисциплин по выбору учебного плана.

Для освоения дисциплины необходимы знания, умения и навыки, сформированные в ходе изучения дисциплин: «Архитектура вычислительных систем», «Физические основы информационных технологий».

В результате освоения дисциплины «Технологии построения систем отображения информации» формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Проектирование информационных систем», «Управление информационными системами», «Моделирование и оптимизация в задачах информатизации гуманитарной сферы», «Управление проектами информационных систем гуманитарной сферы».

2 Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	16
3	Практические работы	26
Всего:		42

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 66 академических часов.

3 Содержание дисциплины «Технологии построения систем отображения информации»

№	Наименование раздела дисциплины	Содержание
1.	Тема 1. Формирование информационных моделей. Основные закономерности восприятия визуальной	Основные принципы формирования и восприятия информационных моделей. Информационная модель и формирование ее элементов. Основные фотометрические

	информации.	параметры. Структура и основные технические параметры средств отображения информации. Цель изучения дисциплины и вопросы организации изучения, литературные источники. Назначение и области применения средств отображения информации. Информационные модели, их виды параметры и характеристики. Информационная емкость информационных моделей в информационном поле. Физиологические особенности восприятия зрительной информации оператором. Зрительный аппарат человека. Законы восприятия визуальной информации. Основы цветового зрения и калориметрические системы, способы смешения цветов.
2.	Тема 2. Принципы телевизионной передачи. Оптико-электрические и электрооптические преобразования в устройствах ТВ и отображения информации.	Виды дискретизации при передаче ТВ-изображений. Виды разверток. Телевизионный сигнал, его характер, временные и спектральные характеристики. Структурная схема ТВ-системы. Полный ТВ-сигнал. Телевизионное изображение и его параметры. Качество ТВ-изображения, виды искажений изображения, способы их оценки. Испытательные сигналы и таблицы. Основные физические процессы в преобразователях изображений и сигналов. Оптико-электрические преобразователи, типы мишеней передающих трубок в ТВ. Классификация передающих трубок, суперортикон и видикон. Преобразователи на основе ПЗС. Электрооптические преобразователи сигналов: на дискретных элементах и непрерывные. Кинескопы черно-белые и цветные. Принципы и устройства отображения на больших экранах. Построение устройств отображения информации на матричных экранах. Виды хранения сигналов изображения.
3.	Тема 3. Основы схемотехники в устройствах ТВ и отображения информации.	Усилители в устройствах отображении информации и ТВ, их структура и функции. Противозумовая коррекция, коррекция апертурных, нелинейных искажений, восстановление постоянной составляющей. Процессы и устройства развертки. Выходные каскады устройств развертки. Особенности прогрессивной и чересстрочной разверток. Процессы и устройства развертки. Выходные каскады устройств развертки. Особенности прогрессивной и чересстрочной разверток. Процессы и устройства синхронизации, цепи синхронизации в ТВ-системах. Методы повышения помехоустойчивости устройств

		синхронизации. Методы генерации символов в устройствах отображения информации. Типовые функциональные схемы этих устройств.
4.	Тема 4. Устройства отображения информации.	Структура систем отображения информации, основные виды функциональных частей отображения информации и их взаимодействие. Основные тактико-технические характеристики устройств отображения информации. Знаковые и графические устройства отображения информации, средства ввода-вывода информации. Основные элементы отображения в устройствах отображения информации, их параметры. Автономные и неавтономные средства. Обзор средств отображения информации старых типов. Новые современные средства отображения информации на основе компьютерных устройств и технологий. Мониторы, панели, табло, индикаторы, дисплеи и видеостены на основе жидкокристаллической (ЖК), плазменной, светодиодной, люминесцентной и лазерной технологий. Проекторы на основе ЖК, лазерной и микрозеркальной технологий. Одно-и многоматричные проекторы.

4 Образовательные технологии.

Занятия лекционного типа.

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов дисциплины «Технологии построения систем отображения информации». На лекциях студенты получают необходимые знания по темам курса. Эти знания полезны в ходе реализации всех остальных видов занятий и в самостоятельной работе студентов.

Чтение лекций сопровождается показом на проекторе иллюстраций, презентаций, видеоматериалов; демонстрацией наглядных пособий: аппаратуры, различных предметов, печатных материалов и пр. Лекции имеют элементы интерактивности: допускается дискуссия, поощряются правильные ответы на вопросы.

Краткие записи лекций, конспектирование помогает усвоить материал. В ходе лекций не ставится задача дословной записи лекций под диктовку преподавателя. Но для подготовки к текущему контролю успеваемости и к промежуточной аттестации на почту студенческой группы высылаются PDF файлы с изложением пройденного материала. Файлы защищены паролем и другими способами, их содержимое не подлежит копированию и редактированию.

Практические занятия в компьютерном классе.

Задачи практических занятий: освоение ПО в области построения систем отображения информации, а затем выполнение самостоятельных работ, предлагаемых преподавателем. Для освоения ПО составлены подробные инструкции по выполнению заданий. Для самостоятельной работы (а иногда и для освоения) имеются образцы того, что должно получиться.

Как правило, новое приложение лучше осваивать в следующей последовательности: базовые настройки, загрузка исходных данных (в виде файла или вручную), обработка данных основными инструментами, применение других эффективных методов. То есть,

надо не просто описывать весь доступный интерфейс, а знакомить с возможностями программы, в ходе выполнения конкретных (лучше идущих из практики) задач.

Развитое, конкурентоспособное программное приложение может содержать сотни, даже свыше тысячи команд. Запомнить и профессионально освоить их за время занятий невозможно, и не нужно. Главное: ознакомиться со спектром возможностей программы. Тогда если в будущем перед человеком встанет нестандартная задача, то он вспомнит, что ее в принципе можно решить. Самостоятельно, а также с привлечением литературы и специалистов, он сможет ее реализовать.

В ходе занятий каждый студент осваивает ПО в естественном для себя темпе, по распечатанной инструкции. Поощряется взаимопомощь, полезная не только не только тому, кого консультируют, но и тому, кто консультирует.

При выполнении практических заданий по любой тематике нужно стремиться к тому, чтобы часть исходных данных произвольно, или по выбору задавалась самим студентом. Тогда точное повторение результатов работы будет невозможным. Полностью одинаковые работы могут получиться только в результате копирования, а не самостоятельно-го выполнения.

Опрос-коллоквиум.

Проводится в устной форме. Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. Опрос обладает большими возможностями воспитательного воздействия преподавателя, т. к. при непосредственном контакте создаются условия для неформального общения со студентом.

Заблаговременно на почту группы отправляются перечень вопросов и материалы для подготовки к коллоквиуму. На контрольном занятии каждому студенту по случайной выборке даётся один из вопросов, при ответе на который он может готовиться не лимитируемое время (но ответить можно только на текущем занятии). При подготовке разрешается пользоваться любыми источниками.

По готовности студент отвечает на выданный ему вопрос, обычно в ходе ответа становится ясен уровень его знаний. Затем преподаватель задает ему вопросы в пределах всей темы, после чего итоговая оценка становится ясна как преподавателю, так и студенту. Такая методика стимулирует студента при подготовке еще раз тщательно повторить весь курс, а не только заданный ему вопрос. Разумеется, преподаватель старается быть предельно объективным и не принимать во внимание характеристики особенности студента, при условии соблюдения норм корректного поведения.

Тестирование.

Преимущественно осуществляется в ходе промежуточной аттестации по дисциплине. Программа тестирования разработана преподавателями из нескольких вузов и опубликована на ресурсе tester.pp.ru. При тестировании каждый студент получает случай-но отобранный блок вопросов, по всем разделам курса, причём номера ответов каждый раз меняются; правильный ответ может оказаться в любой позиции. Это исключает составление «шпаргалки» по тесту. Имеются также развитые средства контроля процесса тестирования и обработки результатов.

Предварительно студентам отправляется список вопросов теста, без ответов, (в том числе и по практической работе в программах). При тестировании студенту даётся 24 вопроса. Время прохождения теста – 45 минут. Для каждого из вопросов теста существует 4 ответа, только один из 4-х правильный. Проходной балл: 50% - удовлетворительно (12-17 правильных ответов), 75 % - хорошо (18-21 правильных ответов), более 90% - отлично (22-24 правильных ответа).

Самостоятельная работа.

Целью самостоятельной (внеаудиторной) работы студентов является обучение навыкам работы с научно-теоретической, периодической, научно-технической литературой и технической документацией, необходимыми для углубленного изучения

дисциплины «Технологии построения систем отображения информации», а также развитие у них устойчивых способностей к самостоятельному изучению и изложению полученной информации. Кроме того, на самостоятельную работу выносятся практические задания, которые студент по тем или иным причинам не выполнил в компьютерном классе.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос	15 баллов	15 баллов
- выполнение практических работ	5 баллов	15 баллов
- контрольная работа в форме компьютерного тестирования	20 баллов	20 баллов
- выполнение домашнего задания	10 баллов	10 баллов
Промежуточная аттестация (Зачет)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А,В	отлично/ зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	хорошо/ зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	удовлетвори- тельно/ зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлетворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Примерные вопросы на компьютерное тестирование:

Компетенция ПК-6: ПК-6.1, ПК-6.2, ПК-6.3

1. Перечислите основные требования к современным системам отображения информации.
2. Перечислите основные параметры СОИ.
3. Назовите два основных класса индикаторных элементов. Какие из них нашли широкое применение в настоящее время?
4. Приведите примеры современных бортовых систем отображения информации выпускаемых отечественными и зарубежными фирмами.
5. Что положено в основу электролюминесценции?
6. Что представляет из себя светодиод?
7. Какая рабочая среда у плазменных УОИ?
8. Какие виды голограмм вы знаете?
9. Какие недостатки присущи голографическим индикаторам?
10. Каким образом достигается свечение в ЖКИ?
11. Перечислите достоинства и недостатки ЖКИ.
12. С какими новыми технологиями в УО вы знакомы?
13. Какие цели преследуются при создании систем индикации?
14. Какие модули программ включает в себя математическое обеспечение УОИ?

Компетенции ПК-8: ОПК-8.1, ПК-8.2, ПК-8.3.

1. Кто является основным ответственным за определение уровня классификации информации?
 - Руководитель среднего звена
 - Высшее руководство
 - Владелец
 - Пользователь
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - Сотрудники
 - Хакеры
 - Атакующие
 - Контрагенты (лица, работающие по договору)
3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
 - Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
 - Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
 - Улучшить контроль за безопасностью этой информации
 - Снизить уровень классификации этой информации
4. Что самое главное должно продумать руководство при классификации данных?
 - Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
 - Необходимый уровень доступности, целостности и конфиденциальности
 - Оценить уровень риска и отменить контрмеры
 - Управление доступом, которое должно защищать данные
5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
 - Владельцы данных
 - Пользователи
 - Администраторы
 - Руководство
6. Что такое процедура?
 - Правила использования программного и аппаратного обеспечения в компании
 - Пошаговая инструкция по выполнению задачи
 - Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
 - Обязательные действия
7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
 - Поддержка высшего руководства
 - Эффективные защитные меры и методы их внедрения
 - Актуальные и адекватные политики и процедуры безопасности
 - Проведение тренингов по безопасности для всех сотрудников
8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
 - Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

- Когда риски не могут быть приняты во внимание по политическим соображениям
 - Когда необходимые защитные меры слишком сложны
 - Когда стоимость контрмер превышает ценность актива и потенциальные потери
9. Что такое политики безопасности?
- Пошаговые инструкции по выполнению задач безопасности
 - Общие руководящие требования по достижению определенного уровня безопасности
 - Широкие, высокоуровневые заявления руководства
 - Детализированные документы по обработке инцидентов безопасности
10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- Анализ рисков
 - Анализ затрат / выгоды
 - Результаты ALE
 - Выявление уязвимостей и угроз, являющихся причиной риска
11. Что лучше всего описывает цель расчета ALE?
- Количественно оценить уровень безопасности среды
 - Оценить возможные потери для каждой контрмеры
 - Количественно оценить затраты / выгоды
 - Оценить потенциальные потери от угрозы в год
12. Тактическое планирование – это:
- Среднесрочное планирование
 - Долгосрочное планирование
 - Ежедневное планирование
 - Планирование на 6 месяцев
13. Что является определением воздействия (exposure) на безопасность?
- Нечто, приводящее к ущербу от угрозы
 - Любая потенциальная опасность для информации или систем
 - Любой недостаток или отсутствие информационной безопасности
 - Потенциальные потери от угрозы
14. Эффективная программа безопасности требует сбалансированного применения:
- Технических и нетехнических методов
 - Контрмер и защитных механизмов
 - Физической безопасности и технических средств защиты
 - Процедур безопасности и шифрования
15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
- Внедрение управления механизмами безопасности
 - Классификацию данных после внедрения механизмов безопасности
 - Уровень доверия, обеспечиваемый механизмом безопасности
 - Соотношение затрат / выгод
16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
- Только военные имеют настоящую безопасность
 - Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
 - Военным требуется больший уровень безопасности, т.к. их риски существенно выше
 - Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?
- Угрозы x Риски x Ценность актива
 - (Угрозы x Ценность актива x Уязвимости) x Риски
 - SLE x Частоту = ALE
 - (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля
18. Что из перечисленного не является целью проведения анализа рисков?
- Делегирование полномочий
 - Количественная оценка воздействия потенциальных угроз
 - Выявление рисков
 - Определение баланса между воздействием риска и стоимостью необходимых контрмер
19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
- Поддержка
 - Выполнение анализа рисков
 - Определение цели и границ
 - Делегирование полномочий
20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
- Чтобы убедиться, что проводится справедливая оценка
 - Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
 - Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
 - Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
21. Что является наилучшим описанием количественного анализа рисков?
- Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
 - Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
 - Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
 - Метод, основанный на суждениях и интуиции
22. Почему количественный анализ рисков в чистом виде не достижим?
- Он достижим и используется
 - Он присваивает уровни критичности. Их сложно перевести в денежный вид.
 - Это связано с точностью количественных элементов
 - Количественные измерения должны применяться к качественным элементам
23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
- Много информации нужно собрать и ввести в программу
 - Руководство должно одобрить создание группы
 - Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
 - Множество людей должно одобрить данные
24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

- Стандарты
 - Должный процесс (Due process)
 - Должная забота (Due care)
 - Снижение обязательств
25. Что такое CobIT и как он относится к разработке систем информационной безопасности и программ безопасности?
- Список стандартов, процедур и политик для разработки программы безопасности
 - Текущая версия ISO 17799
 - Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
 - Открытый стандарт, определяющий цели контроля
26. Из каких четырех доменов состоит CobIT?
- Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
 - Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
 - Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
 - Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
27. Что представляет собой стандарт ISO/IEC 27799?
- Стандарт по защите персональных данных о здоровье
 - Новая версия BS 17799
 - Определения для новой серии ISO 27000
 - Новая версия NIST 800-60
28. CobIT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
- COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
 - COSO относится к стратегическому уровню, тогда как CobIT больше направлен на операционный уровень
 - COSO учитывает корпоративную культуру и разработку политик
 - COSO – это система отказоустойчивости
29. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
- NIST и OCTAVE являются корпоративными
 - NIST и OCTAVE ориентирован на ИТ
 - AS/NZS ориентирован на ИТ
 - NIST и AS/NZS являются корпоративными
30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
- Анализ связующего дерева
 - AS/NZS
 - NIST
 - Анализ сбоев и дефектов.

Вопросы промежуточного контроля (Зачет):

Компетенция ПК-6: ПК-6.1, ПК-6.2, ПК-6.3

1. Способы отображения информации
2. Информационная модель (типы отношений, виды ИМ, параметры ИМ)
3. Фотометрические параметры
4. Психофизиологические особенности восприятия информации: строение зрительного анализатора
5. Основные параметры зрения человека: чувствительность, цветовая чувствительность
6. Пространственные характеристики, временные характеристики
7. Обобщенная структурная схема СОИ, основные параметры СОИ
8. Классификация СОИ
9. Классификация ЭЛТ, конструкция ЭЛТ, характеристики ЭЛТ
10. Фокусирующие системы ЭЛТ: электростатическая, электромагнитная
11. Отклоняющие системы ЭЛТ: электростатическая, электромагнитная
12. Цветные ЭЛТ: с теневой маской, тринитрон
13. Классификация СОИ на ЭЛТ
14. Формирование знаков на экране ЭЛТ, типы растров
15. Телевизионный растр (прогрессивная и чересстрочная развертки)
16. СОИ телевизионного типа (принцип формирования знаков)
17. Буквенно-цифровая СОИ телевизионного типа
18. Графические СОИ телевизионного типа
19. Стандарты видеоконтроллеров
20. Кодирование цветов
21. Структурная схема адаптера
22. Режимы работы видеосистем
23. Микропроцессорные системы отображения информации
24. КЭЛТ: функциональная схема, схема подключения, программирование КЭЛТ
25. КПДП: функциональная схема, схема подключения, режимы работы (формат управляющего слова, словосостояние)
26. ППА: функциональная схема, режимы работы, формат УС
27. ПИТ: функциональная схема, режимы работы, формат УС
28. ПККИ: функциональная схема, схема подключения, программирование ПККИ, словосостояние ПККИ, режимы работы ПККИ
29. Устройство ввода информации (клавиатура)
30. Управление дискретными индикаторами: статическое, динамическое, фазоимпульсное
31. ЖКИ: конструкция, принцип действия и способы управления.
32. ГРИ: конструкция, принцип действия и способы управления.
33. СИД: конструкция, принцип действия и способы управления.
34. ВЛИ: конструкция, принцип действия и способы управления.

Компетенции ПК-8: ПК-8.1, ПК-8.2, ПК-8.3.

1. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
 - Безопасная OECD
 - ISO\IEC
 - OECD
 - CRTED
2. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
 - гаммирования;
 - подстановки;

- кодирования;
 - перестановки;
 - аналитических преобразований.
- Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
- гаммирования;
3. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
- гаммирования;
 - подстановки;
 - кодирования;
 - перестановки;
 - аналитических преобразований.
4. Защита информации от утечки это деятельность по предотвращению:
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
 - воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
 - воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
 - неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
 - несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
5. Защита информации это:
- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
 - преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
 - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
 - совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
 - деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
6. Естественные угрозы безопасности информации вызваны:
- деятельностью человека;
 - ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
 - корыстными устремлениями злоумышленников;
 - ошибками при действиях персонала.
7. Искусственные угрозы безопасности информации вызваны:
- деятельностью человека;
 - ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

- воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
 - корыстными устремлениями злоумышленников;
 - ошибками при действиях персонала.
8. К основным непреднамеренным искусственным угрозам АСОИ относится:
- физическое разрушение системы путем взрыва, поджога и т.п.;
 - перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
 - изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
 - чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
 - неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
9. К посторонним лицам нарушителям информационной безопасности относится:
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
 - персонал, обслуживающий технические средства;
 - технический персонал, обслуживающий здание;
 - пользователи;
 - сотрудники службы безопасности.
 - представители конкурирующих организаций.
 - лица, нарушившие пропускной режим;
10. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п.:
- черный пиар;
 - фишинг;
 - нигерийские письма;
 - источник слухов;
 - пустые письма.
11. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
- черный пиар;
 - фишинг;
 - нигерийские письма;
 - источник слухов;
 - пустые письма.
12. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
- детектор;
 - доктор;
 - сканер;
 - ревизор;
 - сторож.
13. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
- детектор;
 - доктор;
 - сканер;

- ревизор;
 - сторож.
14. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
- детектор;
 - доктор;
 - сканер;
 - ревизор;
 - сторож.
15. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
- детектор;
 - доктор;
 - сканер;
 - ревизор;
 - сторож.
16. Активный перехват информации это перехват, который:
- заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
 - основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
 - неправомерно использует технологические отходы информационного процесса;
 - осуществляется путем использования оптической техники;
 - осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
17. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
- активный перехват;
 - пассивный перехват;
 - аудиоперехват;
 - видеоперехват;
 - просмотр мусора.
18. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
- активный перехват;
 - пассивный перехват;
 - аудиоперехват;
 - видеоперехват;
 - 5.просмотр мусора.
19. Перехват, который осуществляется путем использования оптической техники называется:
- активный перехват;
 - пассивный перехват;
 - аудиоперехват;
 - видеоперехват;
 - просмотр мусора.
20. К внутренним нарушителям информационной безопасности относится:

- клиенты;
- пользователи системы;
- посетители;
- любые лица, находящиеся внутри контролируемой территории;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
- персонал, обслуживающий технические средства.
- сотрудники отделов разработки и сопровождения ПО;
- технический персонал, обслуживающий здание

Практический курс предусматривает проведение следующих работ:

1. Исследование систем отображения информации.
2. Цифровые узлы систем отображения информации.
3. Дискретные индикаторы.

Порядок проведения практических работ описан в разделе 9.1.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Беспалов, Д. А. Операционные системы реального времени и технологии разработки кроссплатформенного программного обеспечения. Часть 1 : учебное пособие / Д. А. Беспалов, С. М. Гушанский, Н. М. Коробейникова ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 139 с. - ISBN 978-5-9275-3367-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1088203> (дата обращения: 27.10.2020). – Режим доступа: по подписке.
2. Федотова, Е. Л. Информационные технологии и системы : учебное пособие / Е. Л. Федотова. - Москва : ФОРУМ : ИНФРА-М, 2020. - 352 с. - (Высшее образование). - ISBN 978-5-8199-0376-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1043098>.
3. Вавренюк А.Б., Курьшева О.К., Кутепов С.В. Операционные системы. Основы UNIX: Учебное пособие / М.:НИЦ ИНФРА-М, 2015. - 184 с.
4. Рудаков А.В. Операционные системы и среды : учебник / — М.: КУРС: ИНФРА-М, 2018. — 304 с.
5. Сидорова-Виснадул Б.Д. Технология разработки программного обеспечения : учеб. пособие / М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 400 с.
6. Григорьев А.А. Методы и алгоритмы обработки данных. Учебное пособие. Москва ИНФРА-М, 2017 – 256 с.

Дополнительная

1. Гвоздева В.А. Информатика, автоматизированные информационные технологии и системы. Учебник/ М.:ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 544 с.
2. Максимов Н.В., Попов И.И. Компьютерные сети: Учебное пособие для студ. учреждений СПО / 6-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 464 с.
3. Безручко В.Т. Информатика (курс лекций). М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 432 с.
4. Федорова Г.Н. Разработка, внедрение и адаптация программного обеспечения отраслевой направленности : учеб. пособие / М. :КУРС :ИНФРА-М, 2017. — 336 с.
5. Шандриков А.С. Стандартизация и сертификация программного обеспечения: Учебное пособие / Мн.: РИПО, 2014. - 304 с.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru

ELibrary.ru Научная электронная библиотека www.elibrary.ru

Электронная библиотека Grebennikon.ru www.grebennikon.ru

Cambridge University Press

ProQuest Dissertation & Theses Global

SAGE Journals

Taylor and Francis

JSTOR

<http://znaniyum.com> – Электронно-библиотечная система.

<http://window.edu.ru> - Информационная система «Единое окно доступа к образовательным ресурсам».

<http://encyclopedia.ru> – онлайн-энциклопедия.

<http://www.informio.ru> – Электронный справочник «Информо» для высших учебных заведений.

<http://www.consultant.ru/> - КонсультантПлюс. Правовая поддержка.

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7 Материально-техническое обеспечение дисциплины.

Для материально-технического обеспечения дисциплины «Технологии построения систем отображения информации» необходимо:

Лаборатория аппаратных средств вычислительной техники – ауд. № 128:

1. 1 компьютер преподавателя,
2. 10 компьютеров обучающихся,
3. маркерная доска,
4. проектор;
5. программное обеспечение:
 - Windows 10 – лицензия: 68526624, без даты.
 - Microsoft office 2010 Pro – лицензия: 49420326, 08.12.2011.
 - Microsoft SQL Server 2008 – лицензия: 46931055, 20.05.2010.
 - Microsoft Visual Professional 2019 – лицензия: 63202190, без даты.
 - Mozilla Firefox 52.8.1 ESR - лицензия: свободный доступ.
 - CorelDrawCS6 – лицензия: 4097188, 17.09.2012.
1. Adobe CS4 Master Collection – лицензия: 21375986, 13.01.2010
2. Платформа ZOOM.

8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным

обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
 - для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9 Методические материалы

9.1 Планы практических занятий.

Практическая работа 1. Тема 2. (4 ч.) Исследование систем отображения информации.

Указания по выполнению заданий:

1. Разработать схему с трафиком информации.
2. Разработать и начертить схему трафика информации с описанием принципа её работы.
3. Изучить основные принципы построения систем отображения информации на плазменных панелях.
4. Вычертить схемы и снять основные фотометрические характеристики плазменных панелей

Практическая работа 2. Тема 3. (4ч.) Цифровые узлы систем отображения информации.

Указания по выполнению заданий:

1. Изучить основы построения полиграммных систем отображения информации.
2. разработка структурных и функциональных схем.
3. полиграммных систем отображения информации.

Практическая работа 3. Тема 4. (6 ч.) Дискретные индикаторы.

Указания по выполнению заданий:

1. Изучить основы построения телевизионных систем отображения информации.
2. Создать функциональную схему систем отображения информации на логических элементах.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Технологии построения систем отображения информации» реализуется на факультете Информационных систем и безопасности кафедрой Информационных технологий и систем.

Цель дисциплины – получение практического опыта управления медиатекой цифровой информации; передачи и размещения цифровой информации; тиражирования мультимедиа контента на съемных носителях информации; осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет.

Задачи дисциплины:

- Формировать медиатеки для структурированного хранения и каталогизации цифровой информации.
- Управлять размещением цифровой информации на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети.
- Тиражировать мультимедиа контент на различных съемных носителях информации.
- Публиковать мультимедиа контент в сети Интернет.
- организовывать собственную деятельность, исходя из цели и способов ее достижения, определенных руководителем.

Дисциплина направлена на формирование следующих компетенций:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)
ПК-6 - Способен настраивать, эксплуатировать и сопровождать информационные системы и сервисы.	ПК-6.1 - Знает методы настройки, порядок и мероприятия по эксплуатации и сопровождению информационных систем и сервисов.
	ПК-6.2 - Умеет организовывать настройку, эксплуатацию и сопровождение информационных систем и сервисов.
	ПК – 6.3 - Владеет навыками управления конфигурацией ИС и сервисов в процессе эксплуатации, решения проблем и консультирования пользователей информационных систем и сервисов.
ПК-8 - Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.	ПК-8.1 - Знает способы организации ИТ-инфраструктуры, методы и приемы управления информационной безопасностью.
	ПК-8.2 - Умеет организовывать ИТ-инфраструктуру предприятия и процессы управления информационной безопасностью.
	ПК-8.3 - Владеет навыками организации ИТ-инфраструктуры и управления информационной безопасностью.

В результате освоения дисциплины, студент должен:

Знать: методы настройки, порядок и мероприятия по эксплуатации и сопровождению информационных систем и сервисов, способы организации ИТ-инфраструктуры, методы и приемы управления информационной безопасностью.

Уметь: организовывать настройку, эксплуатацию и сопровождение информационных систем и сервисов, организовывать ИТ-инфраструктуру предприятия и процессы управления информационной безопасностью.

Владеть: навыками управления конфигурацией ИС и сервисов в процессе эксплуатации, решения проблем и консультирования пользователей информационных систем и сервисов, навыками организации ИТ-инфраструктуры и управления информационной безопасностью.

По дисциплине предусмотрена промежуточная аттестация в форме зачета в 3 семестре.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.