

МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования «Кабардино-Балкарский государственный университет им. Х.М.  
Бербекова» (КБГУ)

ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель ОПОП

\_\_\_\_\_ А.С. Ксенофонов

« \_\_\_\_ » \_\_\_\_\_ 2024 г.

УТВЕРЖДАЮ

Директор ИИИиЦТ

\_\_\_\_\_ З.В. Шомахов

« \_\_\_\_ » \_\_\_\_\_ 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Теория информационной безопасности и методология защиты  
информации

Направление подготовки  
**10.03.01 Информационная безопасность**

Профиль подготовки  
Организация и технология защиты информации

Квалификация (степень) выпускника  
Бакалавр

Форма обучения  
Очная

Нальчик 2024

Рабочая программа дисциплины «Теория информационной безопасности и методология защиты информации» / сост. С.М. Арванова – Нальчик: ФГБОУ КБГУ, 2024. – 29 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность, в 5 семестре, 3 курса.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлениям подготовки 10.03.01 Информационная безопасность, утвержденному приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427, зарегистрированного в Минюсте России 18 февраля 2021 г. N 62548.

## СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....	4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО .....	4
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	4
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ .....	5
5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ .....	8
6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ .....	16
7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....	17
7.1. Нормативно-правовая база.....	17
7.2. Основная литература .....	18
7.3. Дополнительная литература .....	18
7.4. Периодические издания .....	19
7.5. Интернет-ресурсы .....	19
7.6. Современные профессиональные базы данных.....	19
7.7. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы .....	19
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	26

## 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины - изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах. Теория определяется как совокупность основных идей и общих принципов, объединенных в единую систему и обобщенно раскрывающих ту или другую область действительности. Применительно к ИБ теорию следует рассматривать как систему основных идей и положений, общих принципов, необходимых для раскрытия сущности и значения ИБ и выработки методологии ЗИ в компьютерных системах.

Методология ЗИ в компьютерных системах - это учение о структуре, логической организации системы ЗИ, видах, методах и средствах деятельности по обеспечению безопасности защищаемой информации в компьютерных системах.

Задачи дисциплины:

- раскрытие понятийного аппарата в области ИБ и ЗИ в компьютерных системах;
- раскрытие содержательных базовых положений;
- раскрытие современной доктрины ИБ;
- определение целей и принципов ЗИ в компьютерных системах;
- установление факторов, влияющих на ЗИ;
- установление угроз информации в компьютерных системах;
- раскрытие направлений, видов, методов и особенностей деятельности злоумышленников в компьютерной сети и при наличии изолированного компьютера;
- раскрытие назначения, сущности и структуры системы ЗИ в компьютерных системах, системных вопросов защиты программ и данных;
- определение требований к программной и программно-аппаратной реализации средств ЗИ в компьютерных системах и к защите АСУ от несанкционированного доступа (НСД).

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теория информационной безопасности и методология защиты информации» включена в вариативную часть обязательных дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность профиль: Организация и технология защиты информации .

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность жизнедеятельности, Правоведение.

## 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки:

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

- ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

- ПКС-3.3 Способен оценить защищенность объектов информатизации с помощью типовых программных средств.

В результате освоения дисциплины студент должен:

знать:

– принципы работы, связанные с обеспечением комплексной защиты информации на основе существующих программ и методик; основные угрозы информации в компьютерных системах; существующие методы и средства, применяемые для контроля и защиты информации; системные вопросы защиты программ и данных; основные категории требований к программной и программно-аппаратной реализации средств защиты информации; требования к защите автоматизированных систем от НСД.

уметь:

– проводить анализ материалов учреждений, организаций и предприятий отрасли с целью выработки, и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну; анализировать методы и средства контроля и защиты информации и разрабатывать предложения по их совершенствованию и повышению эффективности ЗИ.

владеть:

– нормативными и методическими документами, новыми схемами аппаратуры контроля, средств автоматизации контроля; моделями и системами защиты информации, оценкой технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по ЗИ, аттестации и категорировании объектов защиты.

#### 4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1

№	Наименование раздела	Содержание раздела	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	Основные составляющие информационной безопасности	Цель, задачи, содержание и структура дисциплины. Место дисциплины в системе подготовки специалистов по защите информации. Сущность и понятие ИБ. Значение ИБ и ее место в системе национальной безопасности. Основные составляющие ИБ. Основные принципы обеспечения ИБ. Основные угрозы информационной безопасности РФ. Основные угрозы доступности, целостности и конфиденциальности. Структура органов РФ по обеспечению ИБ.	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)
2	Цели и средства злоумышленников в компьютерных сетях.	Классификация категорий хакеров (злоумышленников) и их целей. Средства НСД в компьютерную систему. Организационно-коммуникативные средства НСД. Технические средства НСД. Программные средства НСД. НСД в сетях.	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)
3	Особенности возникновения угроз защищаемой	Основные сведения об угрозах сетевого взаимодействия. Анализ уязвимости информационных систем. Классификация	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)

	информации в открытых сетях.	сетевых атак. Анализ особенностей организации сетевых атак. Неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС.		
4	Специфика безопасности локальных вычислительных сетей и информационных систем.	Раскрытие и неавторизованная модификация данных и программ. Раскрытие и подмена трафика ЛВС. Разрушение функций ЛВС. Ошибки в программном обеспечении. Контроль удаленных вычислений.	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)
5	Основные программно-технические меры защиты информационных процессов.	Основные понятия программно-технического уровня ИБ. Особенности ИБ современных ИС. Архитектурная безопасность ИС. Структурная схема системы ЗИ в типовой ИС. Основные функции уровней ЗИ в ИС. Дискреционное и мандатное управление доступом к объектам ИС. Подсистема безопасности защищенных версий операционной системы Windows. Аудит событий безопасности в защищенных версиях ОС Windows. Защита информации от НСД в ОС семейства Unix.	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)
6	Основные средства защиты программного обеспечения.	Средства защиты в составе вычислительной системы. Средства защиты с запросом информации. Средства активной защиты ПО. Средства активной защиты ПО.	ОПК-6, ОПК-8, ПКс-3.3	(К), (РК), (Т), (ЛР)

### Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

Таблица 2

Вид работы	Трудоемкость, часы	
	5 семестр	Всего
<b>Общая трудоемкость (в зачетных единицах)</b>	3	3
<b>Контактная работа (в часах):</b>	68	68
<i>Лекции (Л)</i>	34	34
<i>Лабораторные работы (ЛР)</i>		
<i>Практические занятия (ПЗ)</i>	34	34
<b>Самостоятельная работа (в часах):</b>	13	13
Курсовой проект (КП)		
Курсовая работа (КР)		
Самостоятельное изучение разделов	13	13
<b>Подготовка и прохождение промежуточной аттестации</b>	27	27
<b>Вид промежуточной аттестации</b>	экзамен	экзамен

Таблица 3. Лекционные занятия

№ п/п	Тема
1.	Цель, задачи, содержание и структура дисциплины. Место дисциплины в системе подготовки специалистов по защите информации. Сущность и понятие ИБ. Значение ИБ

	и ее место в системе национальной безопасности. Основные составляющие ИБ. Основные принципы обеспечения ИБ. Основные угрозы информационной безопасности РФ. Основные угрозы доступности, целостности и конфиденциальности. Структура органов РФ по обеспечению ИБ.
2.	Классификация категорий хакеров (злоумышленников) и их целей. Средства НСД в компьютерную систему. Организационно-коммуникативные средства НСД. Технические средства НСД. Программные средства НСД. НСД в сетях.
3.	Основные сведения об угрозах сетевого взаимодействия. Анализ уязвимости информационных систем. Классификация сетевых атак. Анализ особенностей организации сетевых атак. Неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС.
4.	Раскрытие и неавторизованная модификация данных и программ. Раскрытие и подмена трафика ЛВС. Разрушение функций ЛВС. Ошибки в программном обеспечении. Контроль удаленных вычислений.
5.	Основные понятия программно-технического уровня ИБ. Особенности ИБ современных ИС. Архитектурная безопасность ИС. Структурная схема системы ЗИ в типовой ИС. Основные функции уровней ЗИ в ИС. Дискреционное и мандатное управление доступом к объектам ИС. Подсистема безопасности защищенных версий операционной системы Windows. Аудит событий безопасности в защищенных версиях ОС Windows. Защита информации от НСД в ОС семейства Unix.
6.	Средства защиты в составе вычислительной системы. Средства защиты с запросом информации. Средства активной защиты ПО. Средства активной защиты ПО.

Таблица 4. Практические занятия

№ Темы	Темы практических занятий
1	Цель, задачи, содержание и структура дисциплины. Место дисциплины в системе подготовки специалистов по защите информации. Сущность и понятие ИБ. Значение ИБ и ее место в системе национальной безопасности. Основные составляющие ИБ. Основные принципы обеспечения ИБ. Основные угрозы информационной безопасности РФ. Основные угрозы доступности, целостности и конфиденциальности. Структура органов РФ по обеспечению ИБ.
2	Классификация категорий хакеров (злоумышленников) и их целей. Средства НСД в компьютерную систему. Организационно-коммуникативные средства НСД. Технические средства НСД. Программные средства НСД. НСД в сетях.
3	Основные сведения об угрозах сетевого взаимодействия. Анализ уязвимости информационных систем. Классификация сетевых атак. Анализ особенностей организации сетевых атак. Неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС.
4	Раскрытие и неавторизованная модификация данных и программ. Раскрытие и подмена трафика ЛВС. Разрушение функций ЛВС. Ошибки в программном обеспечении. Контроль удаленных вычислений.
5	Основные понятия программно-технического уровня ИБ. Особенности ИБ современных ИС. Архитектурная безопасность ИС. Структурная схема системы ЗИ в типовой ИС. Основные функции уровней ЗИ в ИС. Дискреционное и мандатное управление доступом к объектам ИС. Подсистема безопасности защищенных версий операционной системы Windows. Аудит событий безопасности в защищенных версиях ОС Windows. Защита информации от НСД в ОС семейства Unix.
6	Средства защиты в составе вычислительной системы. Средства защиты с запросом информации. Средства активной защиты ПО. Средства активной защиты ПО.

Таблица 5. Самостоятельное изучение разделов дисциплины

№ раздела	Вопросы, выносимые на самостоятельное изучение
-----------	--

1.	Цель, задачи, содержание и структура дисциплины. Место дисциплины в системе подготовки специалистов по защите информации. Сущность и понятие ИБ. Значение ИБ и ее место в системе национальной безопасности. Основные составляющие ИБ. Основные принципы обеспечения ИБ. Основные угрозы информационной безопасности РФ. Основные угрозы доступности, целостности и конфиденциальности. Структура органов РФ по обеспечению ИБ.
2.	Классификация категорий хакеров (злоумышленников) и их целей. Средства НСД в компьютерную систему. Организационно-коммуникативные средства НСД. Технические средства НСД. Программные средства НСД. НСД в сетях.
3.	Основные сведения об угрозах сетевого взаимодействия. Анализ уязвимости информационных систем. Классификация сетевых атак. Анализ особенностей организации сетевых атак. Неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС.
4.	Раскрытие и неавторизованная модификация данных и программ. Раскрытие и подмена трафика ЛВС. Разрушение функций ЛВС. Ошибки в программном обеспечении. Контроль удаленных вычислений.
5.	Основные понятия программно-технического уровня ИБ. Особенности ИБ современных ИС. Архитектурная безопасность ИС. Структурная схема системы ЗИ в типовой ИС. Основные функции уровней ЗИ в ИС. Дискреционное и мандатное управление доступом к объектам ИС. Подсистема безопасности защищенных версий операционной системы Windows. Аудит событий безопасности в защищенных версиях ОС Windows. Защита информации от НСД в ОС семейства Unix.
6.	Средства защиты в составе вычислительной системы. Средства защиты с запросом информации. Средства активной защиты ПО. Средства активной защиты ПО.

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Формы контроля текущих, рубежных и промежуточных знаний студентов по дисциплине определяются в соответствии с учебным планом образовательной программы и в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ.

От обучающихся требуется посещение занятий, выполнение лабораторных работ, знакомство с рекомендованной литературой.

При аттестации обучающихся оценивается качество работы на занятиях (умение вести дискуссию, способность четко и ёмко формулировать свои мысли), уровень подготовки к самостоятельной деятельности, качество выполнения заданий (презентаций, докладов, выполнение лабораторных работ и др.).

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

### 5.1. Оценочные материалы для текущего контроля.

Цель текущего контроля – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины «», оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы

#### Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине «». Развёрнутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.



В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

3 балла	2 балла	1 балл	0 баллов
<p>ставится, если обучающийся:</p> <p>1) полно излагает изученный материал, даёт правильное определенное экономических понятий;</p> <p>2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные;</p> <p>3) излагает материал последовательно и правильно с точки зрения норм литературного языка.</p>	<p>ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.</p>	<p>ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но:</p> <p>1) излагает материал неполно и допускает неточности в определении понятий;</p> <p>2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;</p> <p>3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.</p>	<p>ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.</p>

Баллы «1», «2», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных на протяжении занятия. начисляются в зависимости от сложности задания.

## 5.2. Оценочные материалы для самостоятельной работы обучающегося ( типовые задачи) (при наличии)

Рабочая программа предусматривает проведение лекционных, лабораторных занятий, а также самостоятельную работу обучающихся. В ФГБОУ ВО «Кабардино-Балкарский государственный университет» действует балльно-рейтинговая система оценки учебных достижений, обучающихся по образовательным программам, реализуемым на основании федеральных государственных образовательных стандартов. Балльно-рейтинговая система оценки знаний является одной из составляющих системы управления качеством образовательной деятельности в университете.

### Примерный перечень вопросов на коллоквиум по темам дисциплины (контролируемая компетенция ОПК-6, ОПК-8, ПКС-3.3)

1. Место ИБ в системе национальной безопасности.
2. Основные принципы обеспечения ИБ.
3. Классификация угроз ИБ.
4. Состав и краткая характеристика внутренних и внешних источников угроз ИБ.
5. Сущность и понятие информационной безопасности (ИБ).
6. Характеристика основных составляющих ИБ.

7. Значение ИБ для субъектов информационных отношений.
8. Состав и краткая характеристика основных угроз доступности.
9. Состав и краткая характеристика основных угроз целостности.
10. Состав и краткая характеристика основных угроз конфиденциальности.
11. Классификация категорий хакеров и их целей.
12. Состав и краткая характеристика организационно-коммуникативных средств НСД.
13. Состав и краткая характеристика технических средств НСД.
14. Состав и краткая характеристика программных средств НСД.
15. Характеристика основных угроз ИБ при взаимодействии с Internet. требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet.
16. Классификация сетевых атак.
17. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга.
18. Определение IP-спуфинга и характеристика основных средств защиты от него.
19. Определение атак типа DoS («отказ в обслуживании») и характеристика основных средств защиты от них.
20. Определение парольных атак и характеристика основных средств защиты от них.
21. Определение атак на уровне приложений и типа Man-in-the-Middle и характеристика основных средств защиты от них.
22. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них.
23. Основные методы и условия неавторизованного доступа к ЛВС.
24. Краткая характеристика основных условий НСД к ЛВС.
25. Краткая характеристика основных условий раскрытия данных ЛВС.
26. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения.
27. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС.
28. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях.
29. Основные сервисы безопасности.
30. Основные принципы архитектурной безопасности и их краткая характеристика.
31. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков.
32. Основные функции централизованного управления рисками и администрирования системы безопасности.
33. Основные функции защиты управления приложениями.
34. Основные функции защиты системы сетей.
35. Основные функции защиты конечных пользователей.
36. Классификация средств защиты программного обеспечения и характеристика их основных категорий.
37. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих.
38. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС.
39. Принципы организации и технического исполнения замков защиты и защиты типа «изменение функций».

40. Классификация средства защиты с запросом информации и характеристика их основных составляющих.
41. Назначение и принцип формирования паролей, шифров, сигнатур.
42. Назначение и основные принципы построения аппаратуры защиты.
43. Классификация средств активной защиты и характеристика их основных составляющих.
44. Определение и характеристика основных внутренних средств активной защиты.
45. Определение и характеристика основных внешних средств активной защиты.
46. Классификация средств пассивной защиты и характеристика их основных составляющих.
47. Назначение и основные принципы организации идентификации программ.
48. Назначение и основные принципы построения устройств контроля.
49. Общий состав требований по обеспечению ИБ.
50. Требования к программно-аппаратным средствам.
51. Требования к подсистеме идентификации и аутентификации.
52. Требования к подсистеме управления доступом.
53. Требования к подсистеме протоколирования аудита.
54. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации.
55. Требования к средствам обеспечения целостности.
56. Требования к средствам управления ИБ.
57. Общий состав требований к межсетевому экрану.
58. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД.
59. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД.
60. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД.
61. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД.
62. Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика.

### **Образцы тестовых вопросов (контролируемая компетенция ОПК-6, ОПК-8, ПКС-3.3)**

#### **Полный перечень тестовых заданий представлен в ЭОИС**

1. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
  - a) достоверной
  - b) конфиденциальной
  - c) документированной
  - d) коммерческой тайной
2. По доступности информация классифицируется на
  - a) открытую информацию и государственную тайну
  - b) конфиденциальную информацию и информацию свободного доступа
  - c) информацию с ограниченным доступом и общедоступную информацию
  - d) виды информации, указанные в остальных пунктах
3. К конфиденциальной информации относятся документы, содержащие

- a) информацию о гражданах
  - b) законодательные акты
  - c) "ноу-хау"
  - d) сведения о золотом запасе страны
4. Безопасность информации -
- a) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности
  - b) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус ее хранения, обработки и использования
  - c) события или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации
  - d) состояние защищенности информации хранящаяся и обрабатываемая в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного доступа
5. Запрещено относить к информации ограниченного доступа
- a) информацию о чрезвычайных ситуациях
  - b) информацию о деятельности органов государственной власти
  - c) документы открытых архивов и библиотек
  - d) все, перечисленное в остальных пунктах

### 5.3. Формы и содержание рубежного контроля

Рубежный и промежуточный контроль освоения студентом дисциплины осуществляется в рамках балльно-рейтинговой системы. Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ приведено в таблице 7.

Таблица 7

Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе

№ рейтинговой точки	Коллоквиум	Лаб.практикум	Посещаемость	Тестирование	Итого
1	7	8	3	5	23
2	7	8	3	5	23
3	7	8	4	5	24

Таблица 8

#### Критерии оценки

Вид мероприятия	Критерии оценки	Баллы
Коллоквиум (устный опрос по теме)	- ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике	0-21 балл
Лабораторное занятие	- понимание цели и задач работы - выполнение заданий и обработка результатов - отчет и защита лабораторной работы	0-24 балла

Компьютерное тестирование по разделам дисциплины	Результаты тестирования (Количество баллов = 5*φ, φ - доля правильно отвеченных тестов по теме).	0-15 баллов
Посещение занятий	При более 3 пропусках без уважительной причины занятий аннулируются баллы	0-10 баллов
Зачет	ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике дисциплины в целом	0-30 баллов
Итоговая оценка		0-100 баллов

**Примерный перечень вопросов к зачету  
(контролируемая компетенция ОПК-6, ОПК-8, ПКС-3.3)**

1. Сущность и понятие информационной безопасности (ИБ).
2. Характеристика основных составляющих ИБ.
3. Значение ИБ для субъектов информационных отношений.
4. Место ИБ в системе национальной безопасности.
5. Основные принципы обеспечения ИБ. Классификация угроз ИБ.
6. Состав и краткая характеристика внутренних и внешних источников угроз ИБ.
7. Состав и краткая характеристика основных угроз доступности.
8. Состав и краткая характеристика основных угроз целостности.
9. Состав и краткая характеристика основных угроз конфиденциальности.
10. Классификация категорий хакеров и их целей.
11. Состав и краткая характеристика организационно-коммуникативных средств НСД.
12. Состав и краткая характеристика технических средств НСД.
13. Состав и краткая характеристика программных средств НСД.
14. Характеристика основных угроз ИБ при взаимодействии с Internet. требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet.
15. Классификация сетевых атак.
16. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга.
17. Определение IP-спуфинга и характеристика основных средств защиты от него.
18. Определение атак типа DoS («отказ в обслуживании») и характеристика основных средств защиты от них.
19. Определение парольных атак и характеристика основных средств защиты от них.
20. Определение атак на уровне приложений и типа Man-in—the-Middle и характеристика основных средств защиты от них.
21. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них.
22. Основные методы и условия неавторизованного доступа к ЛВС.
23. Краткая характеристика основных условий НСД к ЛВС.
24. Краткая характеристика основных условий раскрытия данных ЛВС.
25. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения.

26. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС.
27. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях.
28. Основные сервисы безопасности.
29. Основные принципы архитектурной безопасности и их краткая характеристика.
30. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков.
31. Основные функции централизованного управления рисками и администрирования системы безопасности.
32. Основные функции защиты управления приложениями.
33. Основные функции защиты системы сетей.
34. Основные функции защиты конечных пользователей.
35. Классификация средств защиты программного обеспечения и характеристика их основных категорий.
36. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих.
37. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС.
38. Принципы организации и технического исполнения замков защиты и защиты типа «изменение функций».
39. Классификация средства защиты с запросом информации и характеристика их основных составляющих.
40. Назначение и принцип формирования паролей, шифров, сигнатур.
41. Назначение и основные принципы построения аппаратуры защиты.
42. Классификация средств активной защиты и характеристика их основных составляющих.
43. Определение и характеристика основных внутренних средств активной защиты.
44. Определение и характеристика основных внешних средств активной защиты.
45. Классификация средств пассивной защиты и характеристика их основных составляющих.
46. Назначение и основные принципы организации идентификации программ.
47. Назначение и основные принципы построения устройств контроля.
48. Общий состав требований по обеспечению ИБ.
49. Требования к программно-аппаратным средствам.
50. Требования к подсистеме идентификации и аутентификации.
51. Требования к подсистеме управления доступом.
52. Требования к подсистеме протоколирования аудита.
53. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации.
54. Требования к средствам обеспечения целостности.
55. Требования к средствам управления ИБ.
56. Общий состав требований к межсетевому экрану.
57. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД.
58. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД.
59. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД.

60. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД.
61. Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика.
62. Показатели защищенности межсетевых экранов и их краткая характеристика.

## **Контроль курсовых работ**

Курсовые работы не предусмотрены

### **Критерии формирования оценок по промежуточной аттестации**

«зачтено» – получают обучающиеся, которые относительно полно ориентируются в материале, отвечают без затруднений, допускают незначительное количество ошибок. Обучающийся способен к выполнению сложных заданий. Работа выполнена полностью, но имеются не более одной негрубой ошибки и одного недочета, не более трех недочетов. Допускаются незначительные неточности при решении задач, решено 70% задач;

«не зачтено» – получают обучающиеся, которые допускают значительные ошибки. Обучающийся имеет лишь начальную степень ориентации в материале. В работе число ошибок и недочетов превысило норму для оценки 3 или правильно выполнено менее 2/3 всей работы. Обучающийся дает неверную оценку ситуации, решено менее 50% задач.

### **Методические рекомендации для подготовки к зачету**

Зачет в 5-м семестре является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К зачету допускаются студенты, набравшие не менее 36 баллов по итогам текущего и промежуточного контроля. Студенты, набравшие более 61 балла по итогам промежуточного и текущего контроля имеют право на получение зачета автоматом. На зачете студент может набрать от 15 до 30 баллов.

В период подготовки к зачету студенты вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка студента к зачету включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие зачету по темам курса;
- подготовка к ответу на зачетные вопросы.

При подготовке к зачету студентам целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На зачет выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Зачет проводится в устной форме.

При проведении зачета в письменной (устной) форме ведущий преподаватель составляет зачетные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня зачетных вопросов, доведенного до сведения студентов накануне зачетной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный зачет, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего зачет. На подготовку ответа на билет на зачете отводится 20 минут.

При проведении письменного зачета на работу отводится 60 минут.

Результат устного зачета выражается оценками «зачтено» и «не зачтено», дифференцированного устного зачета – оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «зачтено» выставляется, если студент показал при ответе на зачетные вопросы знание основных положений учебной дисциплины, допустил отдельные погрешности и сумел устранить их с помощью преподавателя; знаком с основной литературой, рекомендованной рабочей программой.

Оценка «не зачтено» выставляется, если при ответе на зачетные вопросы выявились существенные пробелы в знании основных положений учебной дисциплины, неумение студента даже с помощью преподавателя сформулировать правильные ответы на вопросы билета.

## 6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ

Общий балл текущего и рубежного контроля складывается из следующих составляющих (приложение 2). Критерием оценки уровня сформированности компетенций в рамках учебной дисциплины в 5 семестре является зачет. Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися. Типовые задания, обеспечивающие формирование компетенции ОПК-5, ОПК-7, ПК-13 представлены в таблице 9.

Таблица 9. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	<u>Знать</u> способы применения системы нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
	<u>Уметь</u> разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
	<u>Владеть</u> навыками определения политики контроля доступа работников к информации ограниченного доступа	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических	<u>Знать</u> : нормативные правовые документы в области информационной безопасности и защиты информации, действующую систему нормативно-правовых актов в области профессиональной деятельности.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)



документов в целях решения задач профессиональной деятельности (ОПК-8).	<u>Уметь:</u> обобщать, анализировать и систематизировать научную информацию в области информационной безопасности.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)
	<u>Владеть:</u> навыками пользования информационно-справочными системами.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)
"Способен применять критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации" (ПКС-13)	<u>Знать:</u> методы осуществления контроля обеспечения уровня защищенности объектов информатизации.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)
	<u>Уметь:</u> оценить защищенность объектов информатизации с помощью типовых программных средств.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)
	<u>Владеть:</u> методикой применения критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.	Типовые оценочные материалы для устного опроса, типовые тестовые задания (раздел 5)

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 7.1. Нормативно-правовая база

1. Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"»
2. Федеральный закон от 05 апреля 2013 г. № 44-ФЗ (ред. от 31.12.2014) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
3. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
4. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
5. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
8. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
9. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
10. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;

12. Трудовой кодекс РФ. Глава 14. «Защита персональных данных работника».

## 7.2. Основная литература

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 с.— Режим доступа: <http://www.iprbookshop.ru/72444.html>.— ЭБС «IPRbooks»
2. Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 169 с.— Режим доступа: <http://www.iprbookshop.ru/67452.html>.— ЭБС «IPRbooks»
3. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: <http://www.iprbookshop.ru/52182.html>.— ЭБС «IPRbooks»
4. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс]: учебное пособие/ Сагдеев К.М., Петренко В.И., Чипига А.Ф.— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 394 с.— Режим доступа: <http://www.iprbookshop.ru/63152.html>.— ЭБС «IPRbooks»
5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/62945.html>.— ЭБС «IPRbooks»

## 7.3. Дополнительная литература

1. Бурькова Е.В. Физическая защита объектов информатизации [Электронный ресурс]: учебное пособие/ Бурькова Е.В.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017.— 158 с.— Режим доступа: <http://www.iprbookshop.ru/71349.html>.— ЭБС «IPRbooks»
2. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/72090.html>.— ЭБС «IPRbooks»
3. Джонс К.Д. Инструментальные средства обеспечения безопасности [Электронный ресурс]/ Джонс К.Д., Шема М., Джонсон Б.С.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 914 с.— Режим доступа: <http://www.iprbookshop.ru/73679.html>.— ЭБС «IPRbooks»
4. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 с.— Режим доступа: <http://www.iprbookshop.ru/74381.html>.— ЭБС «IPRbooks»
5. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: <http://www.iprbookshop.ru/52209.html>.— ЭБС «IPRbooks»

## 7.4. Периодические издания

Перечень периодических изданий, получаемых библиотекой КБГУ:

- Вестник МГУ. Вычислительная математика и кибернетика
- Вестник российского общества информатики и вычислительной техники
- Информатика и образование
- Информационные технологии
- Мир ПК
- Персональный компьютер сегодня
- Программирование
- Информационная безопасность

## 7.5. Интернет-ресурсы

1. <http://fstec.ru/> Федеральная служба по техническому и экспортному контролю
2. <http://www.fsb.ru/> Федеральная служба безопасности
3. <http://clsz.fsb.ru/> Центр по лицензированию, сертификации и защите государственной тайны ФСБ России
4. <http://pravo.gov.ru/> Официальный интернет-портал правовой информации
5. PCI Security Standards Council – <http://www.pcisecuritystandards.org>.
6. Стандарты информационной безопасности в кредитно-финансовой сфере. Стандарты Банка России – <http://www.abiss.ru/doc>
7. Threatpost <https://threatpost> Сайт об информационной безопасности от Kaspersky Lab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как The New York Times и The Wall Street Journal.
8. Security Lab <http://www.securitylab.ru/> Проект компании Positive Technologies. Помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.
9. Anti-Malware <https://www.anti-malware.ru/> Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.
10. Информационная безопасность банков <https://ib-bank.ru/> Отраслевой портал
11. <http://VOID.RU> Сайт VOID.RU представляет собою независимую прессу, освещающую вопросы информационной безопасности - уязвимостей в программном обеспечении, технологий сбора информации, технологий сохранения целостности систем.
12. <http://Security.NNOV.ru> Security.NNOV является одним из наиболее посещаемых Российских ресурсов посвященных информационной безопасности и безопасности IT технологий и доступен как на русском, так и на английском языках.

## 7.6. Современные профессиональные базы данных

1. База данных Science Index (РИНЦ) <http://elibrary.ru>
2. Национальная электронная библиотека РГБ <https://нэб.рф>
3. Крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. [www.scopus.com](http://www.scopus.com)

## 7.7. Методические указания по проведению различных учебных занятий, к курсовому

## **проектированию и другим видам самостоятельной работы**

### ***Методические рекомендации при работе над конспектом во время проведения лекции***

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются 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.

Целесообразно 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 студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

### ***Методические рекомендации при подготовке к коллоквиуму***

- проработать конспекты лекций по вопросам коллоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемым вопросам;
- ответить на вопросы коллоквиума;
- при затруднениях, проконсультироваться с преподавателем.

### ***Критерии оценивания***

<b>Оценка</b>			
<b>неудовлетворительно 2 балла</b>	<b>удовлетворительно 4 балла</b>	<b>хорошо 6 баллов</b>	<b>отлично 8 баллов</b>
Студент не знает значительной части вопросов, допускает существенные ошибки в ответах на вопросы.	Студент поверхностно знает вопросы коллоквиума, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объеме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

### ***Методические рекомендации по организации самостоятельной работы***

Самостоятельная работа (по В.И. Далью «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

- оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;
- широкое внедрение компьютеризированного тестирования;
- совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;
- модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента 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.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разно уровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам 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 студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент 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. Самостоятельная работа студентов предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль

самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

### ***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 необходимо 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 студенту 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 практическим занятиям 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 студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в 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.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

### ***Методические рекомендации по написанию рефератов***

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна

(то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

#### ***Методические рекомендации для подготовки к экзамену:***

Экзамен в 7 семестре является формой итогового контроля знаний и умений, обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой. К экзамену допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзамену включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие экзамену по темам курса;
- подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводится 60 минут.

Результат устного (письменного) экзамена выражается оценками:

***Оценка «отлично» – от 91 до 100 баллов*** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

***Оценка «хорошо» – от 81 до 90 баллов*** – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердые знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

***Оценка «удовлетворительно» – от 61 до 80 баллов*** – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично,



выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

**Оценка «неудовлетворительно» – от 36 до 60 баллов** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины

### ***Методические рекомендации по выполнению лабораторных работ***

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, изучить теоретические сведения к лабораторной работе

2. Выполнение работы. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Сформулировать выводы по проделанной работе.

3. Составление отчета о проделанной работе. К отчету о выполненной работе предъявляются следующие требования:

Отчет должен содержать исчерпывающие данные, как о цели работы, так и о результатах в следующей последовательности:

- Титульный лист
- цель работы
- задание на лабораторную работу для своего варианта
- ответы на контрольные вопросы
- результаты выполнения работы
- выводы по работе.

4. Защита лабораторной работы с представлением отчета. Защита лабораторной работы проходит в форме свободной беседы по теме лабораторной работы.

### ***Методические рекомендации по подготовке к тестированию***

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

### ***Критерии оценивания***

<b>Оценка</b>			
<b>неудовлетворительно 0 баллов</b>	<b>удовлетворительно 3 балла</b>	<b>хорошо 4 балла</b>	<b>отлично 5 баллов</b>
Менее 50 % правильно выполненных заданий.	50-70% правильно выполненных заданий.	71-85% правильно выполненных заданий.	86-100% правильно выполненных заданий.

## **8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **8.1. Требования к материально-техническому обеспечению**

Специализированная аудитория, используемая при проведении занятий лекционного типа №42, №43, №44, №48, №48а, №56, №58 оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы. Лаборатории оснащены необходимым оборудованием: Аппаратно-программный комплекс Sound Cleaner II, ЛГШ 701, АПК «Колибри», АПК «ST 131 Пиранья II», Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др. Междисциплинарная научно-исследовательская лаборатория специальных психофизиологических исследований.

Студенты имеют доступ через Интернет доступ к единому образовательному portalу, где в открытом доступе имеются ресурсы учебно-методической литературы, являющиеся разработками ведущих ВУЗов России.

При проведении занятий лекционного типа, семинарских занятий используются: лицензионное программное обеспечение:

- Продукты MICROSOFT (WINEDUperDVC ALNG UpgrdSAPk MVL A Faculty EES (Корпоративная подписка на продукты Windows операционная система и офис)) ДОГОВОР №10/ЭА-223.
- Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License, ДОГОВОР № 15/ЭА-223.
- Mathlab/Simulink ДОГОВОР №80/ЕЛ-223.
- Adobe Creative Cloud for Teams – All Apps. Лицензии Education Device license для образовательных организаций ДОГОВОР № 15/ЭА-223.
- ABBYY FineReader ДОГОВОР № 15/ЭА-223.
- Антиплагиат ВУЗ ДОГОВОР № 15/ЭА-223.
- файловый менеджер Far Manager.
- 7zip-архиватор.
- Adobe Reader (свободное распространение)

### **8.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;
2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):
  - присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ не визуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;
  - задания для выполнения на экзамене зачитываются ассистентом;
  - письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;
3. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):
  - на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе записывая под диктовку);
  - зачет/экзамен проводится в письменной форме;
4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекты питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).
  - письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
  - по желанию студента экзамен проводится в устной форме.

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

## 9. ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа:

одобрена на 2024/2025 учебный год. Протокол № \_\_\_\_\_ заседания кафедры от  
« \_\_\_\_ » \_\_\_\_\_ 2024 г.

В рабочую программу внесены следующие изменения:

---

---

---

---

---

Разработчик программы \_\_\_\_\_  
Зав. кафедрой \_\_\_\_\_

**Распределение баллов текущего и рубежного контроля**

№п/п	Вид контроля	Сумма баллов			
		Общая сумма	1-я точка	2-я точка	3-я точка
1	Посещение занятий	до 10 баллов	до 3 б.	до 3б.	до 4б.
2	Текущий контроль:	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
3	Рубежный контроль (тестирование и коллоквиум)	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
4	Итого сумма текущего и рубежного контроля	до 70 баллов	до 23б	до 23 б	до 24 б