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 образовательной программы
_____А.С. Ксенофонтов

«30» мая 2023 г.

УТВЕРЖДАЮ

Директор ИИИиЦТ
_____А.Х. Шапсигов

«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направлению подготовки (специальность)
10.03.01 – Информатика и вычислительная техника

Профиль подготовки:
«Информационно-аналитические системы финансового мониторинга»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Нальчик 2023

Рабочая программа дисциплины «Основы управления информационной безопасностью» / сост. Е.А. Акбашева – Нальчик: КБГУ, 2023. – 30с.

Рабочая программа предназначена для преподавания дисциплины «Основы управления информационной безопасностью» базовой части студентам очной формы обучения, по направлению подготовки 10.03.01 – Информационная безопасность, профиль подготовки: Информационно-аналитические системы финансового мониторинга в 7 семестре 4 курса.

Рабочая программа дисциплины составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от «17» ноября 2020 г. №1427 (зарегистрировано в Минюсте России 18 февраля 2021 г. № 62548).

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью дисциплины «Основы управления информационной безопасностью» является изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Для реализации поставленной цели необходимо решить следующие задачи: ознакомление студентов с терминологией управления информационной безопасностью; изучение методов и средств обеспечения информационной безопасности; освоение навыками формирования требований к системе управления ИБ конкретного объекта.

Изучение дисциплины направлено на подготовку специалистов, способных решать задачи профессиональной деятельности в соответствии с профессиональными стандартами:

- 06.032 – «Специалист по безопасности компьютерных систем и сетей»;
- 06.034 – «Специалист по технической защите информации»;
- 06.033 – «Специалист по защите информации в автоматизированных системах».

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к обязательной части Блока 1 Дисциплины (модули) учебного плана по направлению 10.03.01 Информационная безопасность, профиль «Информационно-аналитические системы финансового мониторинга» – Б1.О.13.

Дисциплине «Основы управления информационной безопасностью» предшествуют дисциплины: «Основы информационной безопасности», «Основы управленческой деятельности», «Документоведение».

При освоении дисциплины обучающийся сможет частично продемонстрировать следующие обобщенные трудовые функции **(ОТФ):**

- Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (профессиональный стандарт 06.033 – «Специалист по защите информации в автоматизированных системах», код В, уровень квалификации 6);
- Внедрение систем защиты информации автоматизированных систем (профессиональный стандарт 06.033 – «Специалист по защите информации в автоматизированных системах», код С, уровень квалификации 6);
- Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации (06.034 – «Специалист по технической защите информации», код В, уровень квалификации 6);

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В совокупности с другими дисциплинами профиля «Информационно-аналитические системы финансового мониторинга» дисциплина «Основы управления информационной безопасностью» направлена на формирование следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 10.03.01 – Информационная безопасность (уровень бакалавриата):

УК-3 – способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;

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-10 – способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ПКС-3 – способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

ПКС-4 – способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

УК-3 – способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

Коды и наименования индикаторов достижения компетенции:

УК-3.1 –способен работать в команде, проявлять лидерские качества и умения;

УК-3.2 – способен определять свою роль в социальном взаимодействии и командной работе, учитывая особенности поведения и интересы других участников;

УК-3.3 – способен применить практический опыт участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия.

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

Коды и наименования индикаторов достижения компетенции:

ОПК-6.1 – способен применить систему 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;

ОПК-6.2 – способен разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;

ОПК-6.3 – способен определить политику контроля доступа работников к информации ограниченного доступа.

ОПК-10 – способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Коды и наименования индикаторов достижения компетенции:

ОПК-10.1 – способен конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности;

ОПК-10.2 – способен применять программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях;

ОПК-10.3 – способен принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.

ПКС-3 – Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

Коды и наименования индикаторов достижения компетенции:

ПКС-3.1 – 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-3.2 – способен осуществлять контроль обеспечения уровня защищенности объектов информатизации;

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

ПКС-4 – Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

Коды и наименования индикаторов достижения компетенции:

ПКС-4.1 – способен разрабатывать предложения по совершенствованию системы управления защиты информации;

ПКС-4.2 – способен осуществлять планирование и организацию работы персонала с учетом требований по защите информации;

ПКС-4.3 – способен выработать рекомендации для принятия решения о модернизации системы защиты информации.

В результате освоения дисциплины студенты должны:

знать:

- роль информационной безопасности в обеспечении национальной безопасности.
- общую структуру комплексных систем защиты информации; угрозы информационной безопасности.
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России ФСТЭК России в данной области, способы сбора и проведения анализа исходной информации для проектирования подсистем и средств обеспечения информационной безопасности, методы подбора и поиска информации с применением новейших информационных технологий, цели и задачи технической разведки;
- классификацию технической разведки;
- комплексы и средства радиоразведки;
- средства акустической разведки;
- электронные устройства перехвата информации;
- средства срытого видеонаблюдения и съемки;
- способы доступа к источникам информации без нарушения государственной границы.

уметь**:**

- пользоваться нормативными документами по защите информации, анализировать и оценивать угрозы информационной безопасности объекта информатизации, подбирать и обобщать материалы нормативных, научно -технических и методических источников, осуществлять меры противодействия НСД с использованием различных программных и аппаратных средств защиты, анализировать отечественные и зарубежные стандарты в области компьютерной безопасности для оценки защищенности компьютерных систем, оценивать возможности технических средств разведки по перехвату информации.
- определять основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.
- выявлять угрозы информационной безопасности.

владеть:

- методикой защиты от угроз информационной безопасности.
- представлениями об информационной безопасности как о средстве обеспечения национальной безопасности.
- навыками поиска нормативно-правовой информации, необходимой для профессиональной деятельности, методами формирования требований по ЗИ, методами анализа применимости тех или иных методов и средств технической разведки для получения информации с конкретного объекта, навыками обзора и анализа информации из различных источников.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

В таблице 1 приводится описание содержание 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

Содержание разделов дисциплины «Основы управления информационной безопасностью»

№	Наименование раздела	Содержание раздела	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	Введение	Основные понятия информационной безопасности	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
2	Основы технологии ИБ	Угрозы информационной безопасности в информационных системах.	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
3	Оценочные стандарты	Оценочные стандарты в информационной безопасности	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
4	Стандарты управления	Стандарты управления информационной безопасностью	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
5	СУИБ	Создание СУИБ на предприятии	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
6	Методика оценки рисков	Методика оценки рисков информационной безопасности компании. Методика оценки рисков	УК-3 ОПК-6 ОПК-10 ПКС-3	ДЗ; ЛР; Т; К; Р, КП; РК

		информационной безопасности компании Digital Security.	ПКС-4	
7	Управление рисками	Методики и технологии управления рисками	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
8.	Разработка корпоративной методики анализа рисков	Разработка корпоративной методики анализа рисков	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
9.	Правовые меры обеспечения информационной безопасности	Правовые меры обеспечения информационной безопасности	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
10.	Организационные меры обеспечения безопасности компьютерных информационных систем	Организационные меры обеспечения безопасности компьютерных информационных систем	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
11.	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
12.	Протоколирование и аудит, шифрование, контроль целостности	Протоколирование и аудит, шифрование, контроль целостности	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
13.	Основы управления информационной безопасностью на государственном уровне. Общие принципы и российская практика	Основы управления информационной безопасностью на государственном уровне. Общие принципы и российская практика	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК
14.	Основные понятия информационной безопасности	Основные понятия информационной безопасности	УК-3 ОПК-6 ОПК-10 ПКС-3 ПКС-4	ДЗ; ЛР; Т; К; Р, КП; РК

Общая трудоемкость дисциплины составляет 5 зачетных единицы (180 часов).

Структура дисциплины «Основы управления информационной безопасностью»

Таблица 2

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Вид работы	**Трудоемкость, часы**	
Семестр	**7**	**всего**

Общая трудоемкость (в зачетных единицах)	5	180
Контактная работа (в часах):	**70**	**70**
Лекции (Л)	28	28
Практические занятия (ПЗ)	42	42
Семинарские занятия (СЗ)	–	–
Лабораторные работы (ЛР)	–	–
Самостоятельная работа (в часах):	**83**	**83**
Курсовой проект (КП), Курсовая работа (КР)	28	28
Расчетно-графическое задание (РГЗ)	–	–
Реферат (Р)	–	–
Эссе (Э)	–	–
Самостоятельное изучение разделов	55	55
Контрольная работа (К)	–	–
Подготовка и прохождение промежуточной аттестации (зачета)	27	27
Вид промежуточной аттестации	Экзамен	Экзамен

Таблица 3

Лекционные занятия

№	Наименование раздела	Содержание раздела
1	Введение	Основные понятия информационной безопасности
2	Основы технологии ИБ	Угрозы информационной безопасности в информационных системах.
3	Оценочные стандарты	Оценочные стандарты в информационной безопасности
4	Стандарты управления	Стандарты управления информационной безопасностью
5	СУИБ	Создание СУИБ на предприятии
6	Методика оценки рисков	Методика оценки рисков информационной безопасности компании. Методика оценки рисков информационной безопасности компании Digital Security.
7	Управление рисками	Методики и технологии управления рисками
8	Разработка корпоративной методики анализа рисков	Разработка корпоративной методики анализа рисков
9	Правовые меры обеспечения информационной безопасности	Правовые меры обеспечения информационной безопасности
10	Организационные меры обеспечения безопасности компьютерных информационных систем	Организационные меры обеспечения безопасности компьютерных информационных систем
11	Программнотехнические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом
12	Протоколирование и аудит, шифрование, контроль целостности	Протоколирование и аудит, шифрование, контроль целостности
13	Основы управления информационной безопасностью на государственном уровне. Общие принципы и российская практика	Основы управления информационной безопасностью на государственном уровне. Общие принципы и российская практика
14	Основные понятия информационной безопасности	Основные понятия информационной безопасности

Таблица 4

Практические занятия

№	Наименование тем
1	Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
2	Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия.
3	Внутренние и внешние аудиты ИБ: цели
4	Внутренние и внешние аудиты ИБ: задачи процессов.
5	Внутренние и внешние аудиты ИБ: сходства и различия.
6	Процессы улучшения системы управления ИБ: основные процессы, их взаимосвязь и роль в рамках СУИБ.
7	Корректирующие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
8	Предупреждающие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
9	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства.
10	Документационное обеспечение СУИБ: понятия документа и записи, иерархия документов системы управления ИБ.
11	Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

Таблица 5

Лабораторные работы не предусмотрены

Таблица 6

Самостоятельное изучение разделов дисциплины

№ п/п	**№ п/п Вопросы, выносимые на самостоятельное изучение**
1.	Защита информации организации с помощью технических систем управления доступом
2.	Пути и способы повышения эффективности управления службой защиты информации
3.	Организация и координация работ по защите информации в экономической деятельности
4.	Значение управления конфликтами в системах организации управления
5.	Объекты информатизации, подлежащие обязательной аттестации
6.	Организационно-штатная структура службы защиты информации
7.	Структурная схема службы защиты информации
8.	Анализ системы защиты информации на предприятии

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 заданий 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 «Практикум на ЭВМ», 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 «Практикум на ЭВМ по информационной безопасности». 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
ставится, если обучающийся: 1) полно излагает изученный материал, даёт правильное определенное экономических понятий; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3) излагает материал последовательно и правильно с точки зрения норм литературного языка.	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.	ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но: 1) излагает материал неполно и допускает неточности в определении понятий; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.	ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.

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.

Вопросы, выносимые на коллоквиум

1 точка:

1. Какие основные реквизиты документа вам известны?
2. С какой целью в реквизитах письма ставиться фамилия и телефон исполнителя?
3. Как оформляется циркулярное письмо?
4. Как определяется юридическая сила служебной документации?
5. Понятие и полномочия коллегиальных органов при составлении документации.
6. Понятие формуляра-образца

2 точка:

1. Какова классификация распорядительной документации?
2. Что такое акт и справка?
3. Понятие технологической документации?
4. Что такое трафаретный документ?
5. Что такое организационно-распорядительные документы?
6. Реквизиты делового письма.
7. Обращения и формуляры.

3 точка:

1. Суть делопроизводства?
2. Проект документа?
3. Как оформляется циркулярное письмо?
4. Как определяется юридическая сила служебной документации?
5. Понятие и полномочия коллегиальных органов при составлении документации.
6. Понятие формуляра-образца
7. Понятие персональных данных.
8. Проект документа и приказ понятия и формы конфиденциальных документов
9. Особенности официально-делового стиля при составлении документа.
10. Организация контроля за исполнением конфиденциальных документов.

Примеры тестовых заданий

Примеры тестовых заданий на 1 точку:

I:

S: … информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. - -: Угроза - +: Защита - -: Сохранение

I:

S: В число логических атак на смарт-карты входят: +: отслеживание зависимостей между входными данными операций, выполняемых смарт- картой, и результатами +: использование некорректных входных данных -: нарушение целостности данных, передаваемых смарт-картой

I:

S: В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят: - +:механизм безопасности - -: сервис безопасности

11

- +: контекст безопасности

Примеры тестовых заданий на 2 точку:

I:

S: … безопасности информации в современных системах её обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы). +: Угрозы -: Имитозащита -: Гамирование

I:
S: В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят: +:удостоверение -: билет -: мандат
I:
S: Угрозы безопасности информации в современных системах её обработки определяются умышленными (преднамеренные угрозы) и (непреднамеренные угрозы). +: Естественными -: Ложными -: Неестественными

Примеры тестовых заданий на 3 точку:

I:
S: … - разработка методов подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия - -: Имитозащита - +: Обеспечение аутентификации - -: Обеспечение конфиденциальности I:
S: Осуществление угроз информационной безопасности может быть произведено: через … в органах коммерческих структур, государственного управления, имеющих возможность получения конфиденциальной информации - -: Шпионов - +: Агентурные источники - -: Вредоносных программ
I:
S: Установление градаций важности защиты защищаемой информации (объекта защиты) называют … защищаемой информации - -: Атакой - +: Категорированием - -: Составлением

Вопросы контроля самостоятельной работы студентов

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему.
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.

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.

Критерии формирования оценок по контрольным точкам (контрольные работы; коллоквиум)

(5 баллов) - ставится за работу, выполненную полностью без ошибок и недочетов; обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, решено 100% задач;

(4 балла) – ставится за работу, выполненную полностью, но при наличии в ней не

более одной негрубой ошибки и одного недочета, не более трех недочетов. Обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, допуская незначительные неточности при решении задач, решено 70% задач;

(3 балла) – ставится за работу, если бакалавр правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой. Обучающийся затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, решено 55% задач

(менее 3 баллов) – ставится за работу, если 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.

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 реферата	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;	0-30 баллов

	- системность знаний по тематике дисциплины в целом	
Итоговая оценка		0-100 баллов

Вопросы, выносимые на экзамен
(контролируемые компетенции УК-3, ОПК-6, ОПК-10, ПКС-3, ПКС-4)

1. Основные понятия в области защиты и обработки конфиденциальных документов.
2. Процессный подход к построению СУИБ и циклическая модель PDCA.
3. Цели и задачи, решаемые СУИБ.
4. Стандартизация в области построения СУИБ: сходства и различия стандартов.
5. Стратегии выбора области деятельности СУИБ.
6. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему.
7. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
8. Политика ИБ и политика СУИБ: сходства и различия.
9. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
10. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
11. Анализ рисков ИБ: основные подходы, основные этапы процесса.
12. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
13. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
14. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
16. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
17. Внедрение процессов управления ИБ: этапы и последовательность.
18. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.
19. Функциональная структура и немашинное информационно-документационное обеспечение системы.
20. Автоматизация документационного обеспечения управления.
21. Сущность, преимущества и недостатки смешанной технологической системы обработки и хранения документов.
22. Классификация каналов практической реализации возможных угроз.
23. Предполагаемые рубежи и уровни защиты документопотоков.
24. Понятие "защищенный документооборот", его цели и задачи.
25. Взаимосвязь защищенного документооборота с системами, средствами и методами защиты документированной информации.
26. Выделенный поток конфиденциальных документов и автономная технология их обработки и хранения.
27. Организационные и технологические особенности делопроизводства по конфиденциальным документам.
28. Учет чистых носителей информации, предназначенных для документирования конфиденциальной информации.
29. Периодические и разовые проверки наличия конфиденциальных документов.

30. Поток конфиденциальных документов, не выделенный из общего документопотока, и применяемая технология их обработки и хранения.

31. Уровень конфиденциальности информации и критерии применения выделенной или не выделенной технологии обработки и хранения конфиденциальных документов.

32. Особенности АСОД, предназначенных для обработки конфиденциальных документов. Попытки типизации систем.

33. ТАСОД.

34. Организационное обеспечение защиты потоков документированной информации в АСОД.

35. Принципы, способы и средства защиты технических носителей информации машиночитаемых документов на внемашинных стадиях их обработки, уничтожения и хранения.

36. Назначение и задачи стадии приема и первичной обработки конфиденциальных документов.

37. Типовой состав операций процедуры первичной обработки документов.

38. Первичная обработка поступивших машиночитаемых и аудиовизуальных документов.

39. Назначение и задачи стадии предварительного рассмотрения и распределения поступивших документов.

40. Критерии целесообразности переноса информации поступивших бумажных документов на машинный носитель.

41. Порядок определения рационального маршрута движения документа.

42. Принципы распределения документов между руководителями, структурными подразделениями и специалистами.

43. Функциональная принадлежность документированной информации.

44. Типовой состав операций процедуры распределения поступивших документов.

45. Методика автоматизированного решения задачи "Прокладка маршрута".

46. Правила работы сотрудников службы документации и вычислительного центра с конфиденциальными документами, порядок хранения документов на их рабочих местах.

47. Средства организационной техники, используемые при выполнения рассмотренных стадий, процедур и операций.

48. Назначение и задачи стадии учета поступивших документов.

49. Соотношение учета и регистрации документов. 50. Централизованная и децентрализованная регистрация. Однократность регистрации документа.

Контроль курсовых работ

Примерные темы курсовых работ.

1. Организационные и технологические задачи службы защиты информации

2. Защита информации организации с помощью технических систем управления доступом

3. Пути и способы повышения эффективности управления службой защиты информации

4. Организация и координация работ по защите информации в экономической деятельности

5. Значение управления конфликтами в системах организации управления

6. Объекты информатизации, подлежащие обязательной аттестации

7. Организационно-штатная структура службы защиты информации

8. Структурная схема службы защиты информации

9. Анализ системы защиты информации на предприятии

10. Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации

11. Структура и содержание должностных инструкций сотрудников службы защиты информации

12. Основные направления организации работы службы защиты информации на предприятии

13. Административно-правовые методы управления на защищенных объектах

14. Сравнительный анализ подходов к вопросам управления инцидентами в информационной безопасности в Российской практике

15. Организация и координация работ по защите информации в оборонной сфере

16. Основные принципы, организационная структура и порядок проведения аттестации

17. Координационные задачи и функции службы защиты информации

18. Порядок установления взаимодействия службы защиты информации с подразделениями внешних служб защиты информации

19. Условия и порядок подбора кадров для службы защиты информации

20. Оценка последствий при утрате конфиденциальной информации на предприятии

21. Персональная ответственность за сохранность носителей информации

22. Методы оценки эффективности и качества службы защиты информации

23. Методы защиты конфиденциальной информации на предприятии

24. Система управления информационной безопасностью ARinteg.

25. Принципы построения и оценка уровня безопасности в информационных системах и сетях

26. Анализ критериев для выбора эффективного программного инструмента управления ИТ-инцидентами в компании

Критерии формирования оценок по промежуточной аттестации

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 твердое 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 для подготовки к экзамену

Экзамен в 7-м семестре является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К экзамену допускаются студенты, набравшие не менее 36 баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

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

Подготовка студента 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 студентам 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 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, доведенного до сведения студентов 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 экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 20 минут.

При проведении письменного экзамена на работу отводится 60 минут.

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Максимальная сумма (100 баллов), набираемая студентом по дисциплине, включает две составляющие:

- первая составляющая – оценка регулярности, своевременности и качества выполнения студентом учебной работы по изучению дисциплины в течение периода изучения дисциплины (семестра, или нескольких семестров) (сумма – не более 70 баллов). Баллы, характеризующие успеваемость студента по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ.
- вторая составляющая – оценка знаний студента по результатам промежуточной аттестации (не более 30 –баллов).

Критерием оценки уровня сформированности компетенций в рамках учебной дисциплины «Основы управления информационной безопасностью» является экзамен.

Общий балл текущего и рубежного контроля складывается из следующих составляющих (Приложение).

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Таблица 9

Результаты освоения формирования, подлежащие проверке

Результаты обучения (компетенции)	**Основные показатели оценки результатов обучения**	**Вид оценочного материала, обеспечивающего формирование компетенций**
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	**ИД-1**$_{\text{УК-3}}$ **Знать** методы работы в команде, способы проявлять лидерские качества и умения **ИД-2**$_{\text{УК-3}}$**Уметь** определять свою роль в социальном взаимодействии и командной работе, учитывая особенности поведения и интересы других участников **ИД-3**$_{\text{УК-3}}$ **Владеть** навыками применения практического опыта участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия.	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
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;	**ИД-1**$_{\text{ОПК-6}}$ **Знать** 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 **ИД-2**$_{\text{ОПК- 6}}$ **Уметь** разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации **ИД-3**$_{\text{ОПК-6}}$ **Владеть** навыками определения политики контроля доступа работников к информации ограниченного доступа	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и	**ИД-1**$_{\text{ОПК-10}}$ **Знать** методики использования программных средств для решения практических задач. **ИД-2**$_{\text{ОПК-10}}$ **Уметь** использовать программные средства для решения практических задач. **ИД-3**$_{\text{ОПК-10}}$ **Владеть** навыками использования программных средств для решения практических задач.	Выполнение практических работ Коллоквиум Тестирование (раздел 5)

поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;		
ПКС-3 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	**ИД-1 $_{ПКС-3}$ Знать** Особенности применения критериев оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации **ИД-2 $_{ПКС-3}$ Уметь** Осуществлять контроль обеспечения уровня защищенности объектов информатизации **ИД-3 $_{ПКС-3}$ Владеть** Навыками оценки защищенности объектов информатизации с помощью типовых программных средств	Выполнение практических работ Коллоквиум Тестирование (раздел 5)
ПКС-4 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	**ИД-1 $_{ПКС4}$ Знать** Методы разработки предложений по совершенствованию системы управления защиты информации **ИД-2 $_{ПКС-4}$ Уметь** Осуществлять планирование и организацию работы персонала с учетом требований по защите информации **ИД-3 $_{ПКС-4}$ Владеть** навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации	Выполнение практических работ Коллоквиум Тестирование (раздел 5)

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ 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».

13. Указы и распоряжения Президента Российской Федерации

14. Указ Президента Российской Федерации № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации».

15. Указ Президента Российской Федерации № 537 от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года»;

16. Указ Президента Российской Федерации № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

7.2. Основная литература

1. Анисимов А.А. Менеджмент в сфере информационной безопасности / А.А. Анисимов. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. —http://www.iprbookshop.ru/52182.html

2. Баркалов С.А. Информационная безопасность при управлении техническими системами: учебное пособие / С.А. Баркалов [и др.]. СПб.: Интермедия, 2017. — 528 с. http://www.iprbookshop.ru/68589.html

3. Астахов А.М. Искусство управления информационными рисками/ А.М. Астахов. Саратов: Профобразование, 2017. — 312 с. http://www.iprbookshop.ru/63803.html

4. Бирюков А.Н. Процессы управления информационными технологиями / А.Н. Бирюков. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 263 с. http://www.iprbookshop.ru/52165.html

5. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

7.3.Дополнительная литература

1. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс] : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html

2. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

3. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс] : учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. — Электрон. текстовые данные. — Воронеж: Воронежский Государственный Аграрный Университет им.

Императора Петра Первого, 2015. — 221 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72672.html

4. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html

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. Защищенный документооборот / Сферы применения [Электронный ресурс] – https://www.rutoken.ru/technologies/using/docflow

2. Защищенный документооборот - Digital Design- digdes.ru/products/zaschischenniy-dokumentooborot.

3. Защищенный документооборот - Электронные Офисные Системы - https://www.eos.ru/eos_special_program/eos_vuz

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 отслежива-ния, анализа и визуализации данных. www.scopus.com
4. Самая полная математическая база данных, охватывающая материалы с конца 19 века. zbMath содержит документы, журналы и книги по математике, статистике, инфор-матике, а также машиностроению, физике, естественным наукам и др. www.zbmath.org

(доступ открытый)

7.7. Методические указания по проведению различных учебных занятий и самостоятельной работы

Методические рекомендации по изучению дисциплины для обучающихся

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться с тематическим планом занятий, списком рекомендованной учебной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий, занести в свою рабочую тетрадь темы и сроки проведения семинаров, написания учебных и творческих работ. При изучении дисциплины, обучающиеся выполняют следующие задания: изучают рекомендованную учебную и научную литературу; пишут контрольные работы, готовят доклады и сообщения к лабораторным занятиям; выполняют

самостоятельные творческие работы, участвуют в выполнении практических заданий. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий

Курс изучается на лекциях, лабораторных занятиях, при самостоятельной и индивидуальной работе обучающихся. Обучающийся для полного освоения материала должен не пропускать занятия и активно участвовать в учебном процессе. Лекции включают все темы и основные вопросы теории и практики. Для максимальной эффективности изучения необходимо постоянно вести конспект лекций, знать рекомендуемую преподавателем литературу, позволяющую дополнить знания и лучше подготовиться к лабораторным занятиям.

В соответствии с учебным планом на каждую тему выделено необходимое количество часов лабораторных занятий, которые проводятся в соответствии с вопросами, рекомендованными к изучению по определенным темам. Обучающиеся должны регулярно готовиться к лабораторным занятиям и участвовать в обсуждении вопросов. При подготовке к занятиям следует руководствоваться конспектом лекций и рекомендованной литературой. Тематический план дисциплины, учебно-методические материалы, а также список рекомендованной литературы приведены в рабочей программе

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

Методические рекомендации по подготовке к практическим занятиям

Практические занятия – составная часть учебного процесса, групповая форма занятий при активном участии обучающихся. Практические занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью практических занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы.

Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа обучающихся – способ активного, целенаправленного приобретения обучающимися 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 обучающихся в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит обучающихся 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:

- Проработка учебного материала (по конспектам, учебной и научной литературе);
- Выполнение разноуровневых заданий;
- Работа с тестами и вопросами для самопроверки;
- Выполнение итоговой контрольной работы.

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

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа обучающихся предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости обучающийся может обращаться за консультацией к

преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

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 обучающихся и позволяет кардинальным образом изменить методику преподавания.

Обучающийся может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Обучающийся имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде обучающийся имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет обучающемуся 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 обучающимся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

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

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.

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

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к материально-техническому обеспечению

Специализированные аудитории, используемые при проведении занятий лекционного типа №42, №43, №41, №46, №48 №58 оснащены мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.

Название лаборатории в которых проходят занятия: Лаборатория “Системы контроля и управления доступом”, Лаборатории Технической защиты информации, Лаборатория Криптографической защиты информации, Лаборатория “Защищённой обработки информации в организации”, Лаборатория «Защиты информации в локальных и корпоративных компьютерных сетях» Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др.

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

Для проведения лекционных занятий с компьютерной поддержкой требуется наличие аудитории с проекционным оборудованием.

Во время самостоятельной работы студенты используют компьютерные классы института информатики, электроники и компьютерных технологий, электронные читальные залы КБГУ и домашние компьютеры.

При проведении занятий лекционного типа используются:

лицензионное программное обеспечение:

– Продукты Microsoft (Desktop EducationALNG LicSaPk OLVS Academic Edition Enterprise) подписка (Open Value Subscription);

– Антивирусное программное обеспечение Kaspersky Endpoint Security Стандартный Russian Edition;

– AltLinux (Альт Образование 8);

свободно распространяемые программы:

– Academic MarthCAD License – математическое программное обеспечение,

которое позволяет выполнять, анализировать важнейшие инженерные расчеты и обмениваться ими;

– WinZip для Windows – программ для сжатия и распаковки файлов;

– Adobe Reader для Windows – программа для чтения PDF файлов;

– Far Manager – консольный файловый менеджер для операционных систем семейства Microsoft Windows;

– Academic MarthCAD License – математическое программное обеспечение, которое позволяет выполнять, анализировать важнейшие инженерные расчеты и обмениваться ими.

8.2. 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 (аудитория для самостоятельной работы и коллективного пользования специальными техническими средствами для обучения инвалидов и лиц с ОВЗ в КБГУ, аудитория № 145 Главный корпус КБГУ):

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 невизуального 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 зачете 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, прочитать и оформить задание, в том числе зазачетеписывая 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, объекту 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 зачет 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 2023/2024 учебный год. Протокол № _____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

ПРИЛОЖЕНИЕ

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