МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

ИНСТИТУТ ИНФОРМАТИКИ, ЭЛЕКТРОНИКИ И РОБОТОТЕХНИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы
_____А.С. Ксенофонтов

«___» _____ 2020 г.

УТВЕРЖДАЮ

Директор ИИЭР
_____ Н.В. Черкесова

«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Контроль и безопасность в компьютерных сетях

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
"Организация и технология защиты информации "

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Нальчик 2020

Рабочая программа дисциплины «Контроль и безопасность в компьютерных сетях» / сост. ст. преподаватель Арванова С.М. – Нальчик: ФГБОУ КБГУ, 2020. – 29 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность, в 6 семестре, 3 курса.

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, зарегистрировано в Министерстве юстиции РФ № 1515 от 01.12.2016.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью дисциплины «Контроль и безопасность в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи дисциплины:

- ознакомить студентов с основными понятиями, используемыми при защите информации в компьютерных сетях;
- дать представление об основных угрозах и проблемах защиты сетевых информационных технологий;
- обучить студентов методам защиты информации в сетях различного назначения.

Изучение дисциплины «Контроль и безопасность в компьютерных сетях» должно способствовать получению профессиональных компетентности и кругозора, умению ориентироваться в методах и тенденциях в развитии средств защиты современных компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина включена в вариативную часть обязательных дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность профиль: Организация и технология защиты информации .

Изучение её базируется на следующих дисциплинах: «Сети и системы передачи информации», «Аппаратные средства вычислительной техники».

Дисциплина «Контроль и безопасность в компьютерных сетях» является дисциплиной профессионального цикла.

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:

а) общепрофессиональными (ОПК):

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

б) Выпускник должен обладать следующими профессиональными компетенциями (ПК)

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

В результате изучения дисциплины студенты должны

знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации.
- вероятные угрозы и возможные пути их нейтрализации; основные типы сетевых

топологий, приемы работы в компьютерных сетях; основы администрирования подсистемы информационной безопасности;
- основы организационно – технических мер защиты информации; методики по выполнению работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

уметь:
- применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем.
- оценивать возникающие угрозы и необходимость их устранения; применять приемы работы в компьютерных сетях; выбирать сетевые технологии, программные и аппаратные средства для построения локальных компьютерных сетей по заданным параметрам для организации ИТ-инфраструктуры предприятия; быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты.
- формулировать необходимые организационно – технические меры ЗИ; выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

Владеть:
- навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз, принципами распределения прав и ответственности при организации доступа к объектам.
- навыками администрирования подсистем информационной безопасности объекта защиты; навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта; навыками использования современных аппаратных и программных средств организации сетей ЭВМ; использования ЭВМ в телекоммуникационных системах и локальных сетях; навыками разработки сетевого программного обеспечения.
- методикой защиты от угроз информационной безопасности; способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

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	Безопасность сетезависимых уровней	Основы организации и функционирования вычислительных сетей. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература.	ОПК-7	(К), (РК), (Т), (ЛР)

		Понятие сети ЭВМ. Этапы развития сетей. Критерии классификации вычислительных сетей. Характеристики вычислительных сетей. Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей. Модель ISO OSI. Стандартные стеки коммуникационных протоколов. Технологии обеспечения безопасности в вычислительных сетях.		
		Физический и канальный уровень построения сетей. Физический уровень построения вычислительных сетей. Стандарты кабелей, используемых для построения сетей. Структурированная кабельная система. Беспроводные сети. Канальный уровень построения вычислительных сетей. Методы доступа к разделяемой среде. Методы коммутации. Угрозы безопасности информации, передаваемой в вычислительных сетях, на физическом и канальном уровнях. Методы их нейтрализации.	ОПК-7	(К), (РК), (Т), (ЛР)
		Технологии построения локальных сетей. Стандарты IEEE 802.x. Управление логическим каналом, метод доступа к разделяемой среде CSMA/CD. Форматы кадров технологии Ethernet. Стандарты физической среды технологии Ethernet. Методика расчета сетей Ethernet. Технологии Token Ring, FDDI. Интерфейс Berkley Sockets. Высокоскоростные технологии построения ЛВС: 100VG-AnyLan, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet. Технологии VLAN. Угрозы безопасности информации, передаваемой в локальных вычислительных сетях. Методы их нейтрализации.	ОПК-7, ПК-3, ПК-5	(К), (РК), (Т), (ЛР)
		Сетевой уровень построения сетей. Маршрутизация. Сетевой уровень построения сетей. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях. Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP).	ОПК-7, ПК-3	(К), (РК), (Т), (ЛР)
2		Транспортная подсистема вычислительных сетей. Транспортный	ПК-3	(К), (РК), (Т), (ЛР)

	Безопасность сетенезависимых уровней	уровень построения сетей. Транспортные протоколы в Internet: TCP и UDP. Транспортный уровень построения сетей. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.		
		Уровень приложений. Управление вычислительными сетями. Представительский и прикладной уровни построения сетей ЭВМ. Протоколы прикладного и представительского уровней сети Internet. Управление сетями ЭВМ. Функции протоколов управления сетью. Протоколы управления SNMP и CMIP. Сетевые службы и средства управления.	ПК-3	(К), (РК), (Т), (ЛР)
		Программно-технические средства защиты вычислительных сетей. Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита вычислительных сетей. Криптографические средства защиты информации в вычислительных сетях. Виртуальные частные сети. Протокол SSL. Средства противодействия компьютерным вирусам. Средства организации ложного информационного ресурса в сети. Использование средств защиты информации в вычислительных сетях для обеспечения информационной безопасности информационных систем.	ПК-3, ПК-5	(К), (РК), (Т), (ЛР)

Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

Таблица 2

Вид работы	**Трудоемкость, часы**	
	5 семестр	Всего
Общая трудоемкость (в зачетных единицах)	144	144
Контактная работа (в часах):	90	90
Лекции (Л)	30	30
Лабораторные работы (ЛР)	30	30
Практические занятия (ПЗ)	30	30
Самостоятельная работа (в часах):	54	54
Курсовой проект (КП) Курсовая работа (КР)		
Самостоятельное изучение разделов	54	54

Подготовка и прохождение промежуточной аттестации		
Вид промежуточной аттестации	Экзамен	Экзамен

Таблица 3. Лекционные занятия

№ п/п	Тема
1.	Основы организации и функционирования вычислительных сетей. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие сети ЭВМ. Этапы развития сетей. Критерии классификации вычислительных сетей. Характеристики вычислительных сетей. Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей. Модель ISO OSI. Стандартные стеки коммуникационных протоколов. Технологии обеспечения безопасности в вычислительных сетях.
2.	Физический и канальный уровень построения сетей. Физический уровень построения вычислительных сетей. Стандарты кабелей, используемых для построения сетей. Структурированная кабельная система. Беспроводные сети. Канальный уровень построения вычислительных сетей. Методы доступа к разделяемой среде. Методы коммутации. Угрозы безопасности информации, передаваемой в вычислительных сетях, на физическом и канальном уровнях. Методы их нейтрализации.
3.	Технологии построения локальных сетей. Стандарты IEEE 802.x. Управление логическим каналом, метод доступа к разделяемой среде CSMA/CD. Форматы кадров технологии Ethernet. Стандарты физической среды технологии Ethernet. Методика расчета сетей Ethernet. Технологии Token Ring, FDDI. Интерфейс Berkley Sockets. Высокоскоростные технологии построения ЛВС: 4100VG-AnyLan, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet. Технологии VLAN. Угрозы безопасности информации, передаваемой в локальных вычислительных сетях. Методы их нейтрализации.
4.	Сетевой уровень построения сетей. Маршрутизация. Сетевой уровень построения сетей. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях. Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP).
5.	Транспортная подсистема вычислительных сетей. Транспортный уровень построения сетей. Транспортные протоколы в Internet: TCP и UDP. Транспортный уровень построения сетей. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.
6.	Уровень приложений. Управление вычислительными сетями. Представительский и прикладной уровни построения сетей ЭВМ. Протоколы прикладного и представительского уровней сети Internet. Управление сетями ЭВМ. Функции протоколов управления сетью. Протоколы управления SNMP и CMIP. Сетевые службы и средства управления.
7.	Программно-технические средства защиты вычислительных сетей. Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита вычислительных сетей. Криптографические средства защиты информации в вычислительных сетях. Виртуальные частные сети. Протокол SSL. Средства противодействия компьютерным вирусам. Средства организации ложного информационного ресурса в сети. Использование средств защиты информации в вычислительных сетях для обеспечения информационной безопасности информационных систем.

Таблица 4. Лабораторные занятия

№ Темы	Темы лабораторных занятий
1.	АУДИТ БЕЗОПАСНОСТИ ПРОТОКОЛА SNMP
2.	АУДИТ БЕЗОПАСНОСТИ ПРОТОКОЛА STP
3.	ВИРТУАЛЬНЫЕ СЕТИ IEEE 802.1Q
4.	БАЗОВЫЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ КОММУТАТОРОВ
5.	БЕЗОПАСНОСТЬ НА ОСНОВЕ ТЕХНОЛОГИИ СЕГМЕНТАЦИИ ТРАФИКА
6.	БЕЗОПАСНОСТЬ НА ОСНОВЕ ПРОТОКОЛА IEEE 802.1X
7.	СПИСКИ КОНТРОЛЯ ДОСТУПА ACL
8.	КОНТРОЛЬ ДОСТУПА К КОММУТАТОРУ
9.	ШИФРОВАНИЕ КАНАЛА С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА WEP
10.	ШИФРОВАНИЕ БЕСПРОВОДНОГО КАНАЛА WI-FI С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛОВ WPA, WPA-2
11.	АУТЕНТИФИКАЦИЯ БЕСПРОВОДНЫХ КЛИЕНТОВ НА ОСНОВЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ И АППАРАТНЫХ АДРЕСОВ КОМПЬЮТЕРОВ
12.	ОБНАРУЖЕНИЕ АТАК ДИССОЦИАЦИИ С ИСПОЛЬЗОВАНИЕМ ОС LINUX
13.	ПРОТОКОЛ PPPOE
14.	ТЕХНОЛОГИЯ NETWORK ADDRESS TRANSLATION (NAT)
15.	ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ VPN
16.	УТИЛИТА IPTABLES
17.	ЦИФРОВЫЕ СЕРТИФИКАТЫ
18.	СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ SNORT
19.	ТУНЕЛЛИРОВАНИЕ СОЕДИНЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА SSL
20.	УДАЛЕННОЕ УПРАВЛЕНИЕ ПО ПРОТОКОЛУ SSH

Таблица 5. Самостоятельное изучение разделов дисциплины

№ раздела	**Вопросы, выносимые на самостоятельное изучение**
2	Основы организации и функционирования вычислительных сетей. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие сети ЭВМ. Этапы развития сетей. Критерии классификации вычислительных сетей. Характеристики вычислительных сетей. Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей. Модель ISO OSI. Стандартные стеки коммуникационных протоколов. Технологии обеспечения безопасности в вычислительных сетях.
3	Физический и канальный уровень построения сетей. Физический уровень построения вычислительных сетей. Стандарты кабелей, используемых для построения сетей. Структурированная кабельная система. Беспроводные сети. Канальный уровень построения вычислительных сетей. Методы доступа к разделяемой среде. Методы коммутации. Угрозы безопасности информации, передаваемой в вычислительных сетях, на физическом и канальном уровнях. Методы их нейтрализации.

4	Технологии построения локальных сетей. Стандарты IEEE 802.x. Управление логическим каналом, метод доступа к разделяемой среде CSMA/CD. Форматы кадров технологии Ethernet. Стандарты физической среды технологии Ethernet. Методика расчета сетей Ethernet. Технологии Token Ring, FDDI. Интерфейс Berkley Sockets. Высокоскоростные технологии построения ЛВС: 4100VG-AnyLan, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet. Технологии VLAN. Угрозы безопасности информации, передаваемой в локальных вычислительных сетях. Методы их нейтрализации.
5	Сетевой уровень построения сетей. Маршрутизация. Сетевой уровень построения сетей. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях. Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP).
6	Транспортная подсистема вычислительных сетей. Транспортный уровень построения сетей. Транспортные протоколы в Internet: TCP и UDP. Транспортный уровень построения сетей. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.
7	Уровень приложений. Управление вычислительными сетями. Представительский и прикладной уровни построения сетей ЭВМ. Протоколы прикладного и представительского уровней сети Internet. Управление сетями ЭВМ. Функции протоколов управления сетью. Протоколы управления SNMP и CMIP. Сетевые службы и средства управления.
8	Программно-технические средства защиты вычислительных сетей. Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита вычислительных сетей. Криптографические средства защиты информации в вычислительных сетях. Виртуальные частные сети. Протокол SSL. Средства противодействия компьютерным вирусам. Средства организации ложного информационного ресурса в сети. Использование средств защиты информации в вычислительных сетях для обеспечения информационной безопасности информационных систем.

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
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.

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

1. Концепция информационной безопасности.
2. Основы экономической безопасности предпринимательской деятельности.
3. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
5. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
6. Информационная безопасность (по материалам зарубежных источников и литературы).
7. Правовые основы защиты конфиденциальной информации.
8. Экономические основы защиты конфиденциальной информации.
9. Организационные основы защиты конфиденциальной информации.
10. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
11. Концепция информационной безопасности.
12. Основные виды угроз информационным ресурсам
13. Особенности угроз конфиденциальной информации
14. Причины возникновения угроз утраты или утечки конфиденциальной информации
15. Причины возникновения каналов несанкционированного доступа к информации
16. Классификация видов каналов несанкционированного доступа к информации
17. Технические каналы несанкционированного доступа к информации
18. Легальные и нелегальные методы обеспечения действия каналов утечки информации
19. Особенности угроз автоматизированным информационным системам
20. Классификация удаленных атак
21. Основные направления правовой защиты информации
22. Схема каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети
23. Степень опасности каналов утечки информации в ЛВС.
24. Элементы программно-технической защиты информационных ресурсов
25. Технические средства защиты информации при проведении вебинаров.

Образцы тестовых заданий

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 хранимая 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

Экзамен	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

Вопросы, выносимые на экзамен (контролируемые компетенции ОПК-7, ПК-3, ПК-5)

1. Понятие и классификация атак на компьютерные сети.
2. Основные типы сетевых атак. Средства реализации атак.
3. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
4. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
5. Технологии обнаружения компьютерных атак и их возможности.
6. Прямые и косвенные признаки атак. Методы обнаружения атак.
7. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак.
8. Стратегии и средства межсетевого экранирования.
9. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
10. Требования руководящих документов ФСТЭК России к межсетевым экранам.
11. Обзор документов RFC, регламентирующих использование межсетевых экранов.
12. Типы межсетевых экранов. Схемы межсетевого экранирования.
13. Фильтрация пакетов. Критерии и правила фильтрации.
14. Реализация пакетных фильтров. Понятие демилитаризованной зоны.
15. Организация узлов для отвлечения внимания злоумышленника.
16. Особенности фильтрации различных типов трафика.
17. Шлюзы прикладного уровня.
18. Контроль HTTP-трафика и электронной почты.
19. Безопасность на первом сетевом уровне.
20. Безопасность стандарта 802.11.
21. Безопасность стандарта 802.15.
22. Безопасность стандарта 802.16 и частных каналов беспроводной передачи данных на высоких частотах.
23. Безопасность спутниковой передачи данных от перехвата и несанкционированного доступа.
24. Операции и безопасность SSH.
25. Операции и безопасность SSL/TLS.
26. Операции и безопасность IPSec.
27. Параметры безопасности, протоколы и режимы функционирования.
28. Выбор шифров и имплементаций.
29. Протоколы аутентификации: RADIUS, TACACS+ и Kerberos.
30. Выбор необходимой имплементации. Уязвимости Kerberos 4.
31. Стандарт аутентификации 802.1x и типы расширяемого протокола аутентификации (EAP).
32. Уязвимости отдельных типов EAP
33. Общие сведения о технологии терминального доступа.
34. Задачи, решаемые VPN. Туннелирование в VPN.
35. Защита данных на канальном уровне.
36. Организация VPN средствами протокола PPTP.
37. Защита данных на сетевом уровне. Протокол SKIP.
38. Протокол IPSec. Защита на транспортном уровне.
39. Настройка SSL-соединения. Организация VPN прикладного уровня.

40. Защищенный обмен электронной почтой.
41. Служба каталогов LDAP.
42. Система единого входа в сеть на основе протокола Kerberos.
43. Создание единого пространства безопасности на базе Active Directory.
44. Защита средствами файловых систем.
45. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.
46. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности.
47. Выявление и построение схемы информационных потоков защищаемой информации.
48. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP.
49. Применение систем автоматизированного построения схемы сети.
50. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети.
51. Применение средств анализа защищенности серверов приложений.
52. Оценка риска обнаруженных уязвимостей.
53. Составление рекомендаций по устранению обнаруженных уязвимостей.
54. Написание и формат отчета об аудите безопасности.
55. Применение средств автоматизации комплексного аудита информационной безопасности.
56. Структура и функции комплексных экспертных систем аудита безопасности.
57. Учет структуры аппаратно-программных средств объекта информатизации.
58. Преимущества и недостатки использования автоматизированных систем проверки безопасности.

Контроль курсовых работ

Курсовые работы не предусмотрены

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 8-м семестре является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К з\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

Общий балл текущего и рубежного контроля складывается из следующих составляющих (приложение 2). Критерием оценки уровня сформированности компетенций в рамках учебной дисциплин в 8 семестре является экзамен. Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися. Типовые задания, обеспечивающие формирование компетенции ПК-1, ОК-8, ПК-15 представлены в таблице 9.

Таблица 9. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности	*Знать:* цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)

информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации.	
	Уметь: применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Владеть: навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз, принципами распределения прав и ответственности при организации доступа к объектам.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	*Знать:* вероятные угрозы и возможные пути их нейтрализации; основные типы сетевых топологий, приемы работы в компьютерных сетях; основы администрирования подсистемы информационной безопасности;	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Уметь: оценивать возникающие угрозы и необходимость их устранения; применять приемы работы в компьютерных сетях; выбирать сетевые технологии, программные и аппаратные средства для построения локальных компьютерных сетей по заданным параметрам для организации ИТ-инфраструктуры предприятия; быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Владеть: навыками администрирования подсистем информационной безопасности объекта защиты; навыками проектирования архитектуры	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)

	системы защиты информации, для обеспечения информационной безопасности объекта; навыками использования современных аппаратных и программных средств организации сетей ЭВМ; использования ЭВМ в телекоммуникационных системах и локальных сетях; навыками разработки сетевого программного обеспечения.	
способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	*Знать:* основы организационно – технических мер защиты информации; методики по выполнению работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Уметь: формулировать необходимые организационно – технические меры ЗИ; выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Владеть: методикой защиты от угроз информационной безопасности; способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;	Коллоквиум Выполнение и защита лабораторных работ Тестирование (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».
13. Указ Президента Российской Федерации № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации».
14. Указ Президента Российской Федерации № 537 от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года»;
15. 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»;
16. Указ Президента Российской Федерации № 1576 от 01 ноября 2008 года «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»;
17. Указ Президента Российской Федерации № 1085 от 16 августа 2004 года «Вопросы Федеральной Службы по техническому и экспортному контролю» (в ред. Указов Президента РФ от 22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321, от 23.10.2008 № 1517, от 17.11.2008 № 1625);
18. Указ Президента Российской Федерации № 960 от 11 августа 2003 года «Вопросы Федеральной Службы Безопасности Российской Федерации» (в ред. Указов Президента РФ от 11.07.2004 № 870, от 31.08.2005 № 1007, от 01.12.2005 № 1383, от 12.06.2006 № 602, от 27.07.2006 № 799, от 28.12.2006 № 1476, от 28.11.2007 № 1594, от 28.12.2007 № 1765, от 01.09.2008 № 1278, от 23.10.2008 № 1517, от 17.11.2008 № 1625, от 22.04.2010 № 499, от 14.05.2010 № 589);
19. Распоряжение Президента Российской Федерации № 366-рп от 10 июля 2001 года «О подписании конвенции о защите физических лиц при автоматизированной обработке персональных данных»

7.2.Основная литература

1. Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 80 с.— Режим доступа: http://www.iprbookshop.ru/74382.html.— ЭБС «IPRbooks»
2. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс]: учебно-методическое пособие/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 218 с.— Режим доступа: http://www.iprbookshop.ru/77317.html.— ЭБС «IPRbooks»
3. 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»
4. Голиков А.М. Кодирование в телекоммуникационных системах [Электронный ресурс]: учебное пособие для специалитета: 090302.65 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, задание на самостоятельную работу/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2016.— 338 с.— Режим доступа: http://www.iprbookshop.ru/72111.html.— ЭБС «IPRbooks»

7.3.Дополнительная литература

1. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 782 c.— Режим доступа: http://www.iprbookshop.ru/72337.html.— ЭБС «IPRbooks»
2. 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 c.— Режим доступа: http://www.iprbookshop.ru/73679.html.— ЭБС «IPRbooks»
3. Чуянов А. Г. Проблемы защищенности телекоммуникационных систем [Электронный ресурс]: учебное пособие/ Чуянов А. Г.— Электрон. текстовые данные.— Омск: Омская академия МВД России, 2015.— 164 c.— Режим доступа: http://www.iprbookshop.ru/61873.html.— ЭБС «IPRbooks»
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей –М.: Форум: Инфра-М, 2013.-592с.

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://all-ib.ru/
2. http://SecurityLab.ru
3. http://infosecurity.report.ru/
4. https://nordrus.info/security/
5. http://www.anti-malware.ru/

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

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

Оценка			
неудовлетворительно 2 балла	**удовлетворительно 4 балла**	**хорошо 6 баллов**	**отлично 8 баллов**
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. Далю «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 экзамен 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 отводиться 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 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 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

Оценка			
неудовлетворительно 0 баллов	**удовлетворительно 3 балла**	**хорошо 4 балла**	**отлично 5 баллов**
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 №46, №48, №48а, №50, №56, №58 оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.
Лаборатории оснащены необходимым оборудованием: Комплект учебного оборудования ПО 1715 «Локальные компьютерные сети», Комплект учебного оборудования ПО 1154 «Корпоративные компьютерные сети», Комплект учебного оборудования ПО 1582 «Глобальные компьютерные сети», Комплект учебного оборудования ПО 1305 «Сетевая безопасность», Комплект учебного оборудования ПО 1092 «Беспроводные сети Wi-Fi», Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др. Лаборатория «Защищенной обработки информации сетевых технологий Cisco»

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

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:

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 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, прочитать 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, 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 экзамен проводится в устной форме.

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

Лист переутверждения рабочей программы дисциплины

Рабочая программа:

одобрена на 2020/2021 учебный год. Протокол № __ заседания кафедры от «__» __ 2020 г.

Разработчик программы_____
Зав. кафедрой_____