МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заместитель директора по УМР

_____ Н.В. Зонова

«_____» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Защита информации**

направление подготовки: **09.03.01 Информатика и вычислительная техника**

направленность (профиль): **Автоматизированные системы обработки информации и управления**

форма обучения: **очная, заочная**

Рабочая программа разработана для обучающихся по направлению подготовки 09.03.01 «Информатика и вычислительная техника», направленность (профиль) «Автоматизированные системы обработки информации и управления»

Рабочая программа рассмотрена
на заседании кафедры кибернетических систем

Заведующий кафедрой О.Н. Кузяков

Рабочую программу разработал:

А.М. Андриянов, доцент кафедры кибернетических систем, к.т.н, доцент _____

1. Цели и задачи освоения дисциплины

Цель дисциплины:

ознакомление обучающихся с аппаратными и программными средствами защиты компьютерной информации и с защитой информационных процессов в компьютерных сетях.

Задачами дисциплины являются:

–изучение современных методов и средств защиты информации в компьютерных системах и сетях;

–приобретений практических навыков по применению полученных знаний для защиты компьютерной информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам обязательной части Блока 1 учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знание

- структур и принципов организации операционных систем;
- основ администрирования вычислительных сетей;
- основ управления базами данных;
- эталонной модели взаимодействия открытых систем.

умение

- применять методы настройки и эксплуатации операционных систем, вычислительных сетей и баз данных.

Владение:

- технологиями проверки возможности подключения, установки и проверки функционирования программно-аппаратных средств;
- технологиями инсталляции программного обеспечения для поддержки работы пользователей;
- методикой оценки производительности приложений и методами планирования требуемой производительности**;**
- технологиями регламентного обслуживания оборудования.

Содержание дисциплины является логическим продолжением содержания дисциплин Программирование, Алгоритмы и структуры данных, Объектно–ориентированное программирование, Правовая культура, Формальные языки и теория автоматов, Параллельные методы и алгоритмы, Цифровая схемотехника, Организация ЭВМ, Цифровые технологии, Сетевые технологии, Вычислительные системы, Операционные системы, Сети и телекоммуникации, Системное программное обеспечение, Основы научных исследований в области информационных систем и технологий.

Изучение дисциплины служит основой для выполнения ВКР.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине (модулю)

ОПК-1. Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1. Обладает фундаментальными знаниями, полученными при изучении математических, естественнонаучных и общеинженерных дисциплин, методами теоретического и экспериментального исследования и применяет их при решении стандартных задач профессиональной деятельности.	Знать: З1 – фундаментальные основы из области естественнонаучных и общеинженерных дисциплин, относящиеся к защите информации..
		Уметь: У1–применять фундаментальные знания из области естественнонаучных и общеинженерных дисциплин при защите автоматизированных систем.
		Владеть:В1-методами теоретического и экспериментального исследования защищенности автоматизированных систем.
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.1. Обладает знаниями современных информационных технологий и программных средств, методов их использования, демонстрирует навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Знать: З2 - современные информационные технологии и программные средства в области защиты информационных систем.
		Уметь: У2 – использовать современные информационные технологии и программные средства, в том числе отечественного производства, в области защиты информации.
		Владеть: В2 - навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, в области защиты информации.
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Демонстрирует знание принципов информационной и библиографической культуры, способность применять методы поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, применяет методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	Знать: З3 – принципы информационной и библиографической культуры в области защиты информации.
		Уметь: У3 - применять методы поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций.
		Владеть: В3 - методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры,

		с учетом соблюдения авторского права и требований информационной безопасности.

4. Объем дисциплины «Защита информации»

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/8	22	12	12	26	36	Экзамен
заочная	5/летняя сессия	8	4	6	81	9	Экзамен, контрольная работа

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины/модуля		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в курс.	2	0	0	2	4	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
2	2	Источники, риски и формы атак на информацию	4	0	0	2	6	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
3	3	Криптографические модели, алгоритмы шифрования.	4	4	4	2	14	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчет по лабораторным работам, отчет по практическим заданиям
4	4	Политика безопасности, стандарты безопасности.	2	0	0	20	22	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
5	5	Защита данных в операционных системах	4	4	4	0	12	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчет по лабораторным работам,

									отчет по практическим заданиям
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях.	6	4	4	0	14	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчет по лабораторным работам, отчет по практическим заданиям
7	Экзамен		0	0	0	0	36	ОПК-1.1 ОПК-2.1 ОПК-3.1	Тест
Итого:			22	12	12	26	108		

заочная форма обучения (ЗФО)

Таблица 5.1.2

№ п/п	Структура дисциплины/модуля		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в курс.	1	0	0	4	5	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
2	2	Источники, риски и формы атак на информацию	1	0	0	4	5	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
3	3	Криптографические модели, алгоритмы шифрования.	4	4	2	20	30	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчеты по лабораторным работам, отчет по контрольной работе отчет по практическим заданиям
4	4	Политика безопасности, стандарты безопасности.	0	0	0	20	20	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос
5	5	Защита данных в операционных системах	1	0	2	20	23	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчет по контрольной работе отчет по практическим заданиям
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях.	1	0	2	13	16	ОПК-1.1 ОПК-2.1 ОПК-3.1	Устный опрос, отчет по контрольн

									ой работе отчет по практическим заданиям
7	Экзамен		0	0	0	0	9	ОПК-1.1 ОПК-2.1 ОПК-3.1	Тест
Итого:			8	4	6	81	108		

Очно-заочная форма **не предусмотрена.**

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Введение в курс.

Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.

Раздел 2. Источники, риски и формы атак на информацию.

Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС.

Раздел 3. Криптографические модели, алгоритмы шифрования.

Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы электронной цифровой подписи (ЭЦП).

Раздел 4. Политика безопасности, стандарты безопасности. Понятие политики безопасности, основные типы политики безопасности. Дискреционная и мандатная модели безопасности. Концепция защиты средств вычислительной техники и АС от НСД. Классификация АС и требования по защите информации. Классы и группы защищенности средств вычислительной техники и АС от НСД и требования к ним. Нормативно-правовые документы РФ в области информационной безопасности.

Раздел 5. Защита данных в операционных системах

Модели безопасности и типовая архитектура подсистемы защиты операционной системы, основные функции. Разграничение доступа к объектам операционной системы, идентификация, аутентификация, авторизация субъектов доступа. Аудит. Основные компоненты системы безопасности ОС на примере семейств ОС Windows / Unix.

Раздел 6. Многоуровневая защита корпоративных сетей; защита информации в сетях.

Многоуровневая зашита корпоративных сетей. Сетевые протоколы защиты информации. Сканирование и мониторинг информационной безопасности.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	2	1	-	Введение в курс.
2	2	4	1	-	Источники, риски и формы атак на информацию
3	3	4	4	-	Криптографические модели, алгоритмы шифрования.
4	4	2	0	-	Политика безопасности, стандарты безопасности.

5	5	4	1	-	Защита данных в операционных системах
6	6	6	1	-	Многоуровневая защита корпоративных сетей; защита информации в сетях.
Итого:		22	8	-	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	3	4	4	-	Криптографические системы и протоколы.
2	5	4	0	-	Модели безопасности и типовая архитектура подсистемы защиты операционной системы, основные функции. Основные компоненты системы безопасности ОС на примере семейств ОС Windows / Unix.
3	6	4	0	-	Многоуровневая защита корпоративных сетей. Сетевые протоколы защиты информации.
Итого:		12	4	-	

Лабораторные работы

Таблица 5.2.3

№ п/п	Номер раздела дисциплины				Наименование лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	3	4	2	-	Лабораторная работа № 1. Основы теории чисел
2	5	4	2	-	Лабораторная работа № 2. Криптографические системы
3	6	4	2	-	Лабораторная работа №3. Лабораторная работа № 3. Реализация алгоритма ЭЦП El Gamal
Итого:		12	6	-	

Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины				Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	2	4	-	Введение в курс.	Подготовка к лабораторным и практическим занятиям, оформление отчетов.
2	2	2	4	-	Источники, риски и формы атак на информацию	Подготовка к лабораторным и практическим занятиям, оформление отчетов.
3	3.	2	20	-	Криптографические модели, алгоритмы шифрования.	Подготовка к лабораторным и практическим занятиям, оформление отчетов.
4	4.	20	20	-	Политика безопасности, стандарты безопасности.	Подготовка к лабораторным и

						практическим занятиям, оформление отчетов.
5	5	0	20	-	Защита данных в операционных системах	Подготовка к лабораторным и практическим занятиям, оформление отчетов. Выполнение контрольной работы.
6	6	0	13	-	Многоуровневая защита корпоративных сетей; защита информации в сетях.	Подготовка к лабораторным и практическим занятиям, оформление отчетов. Выполнение контрольной работы.
Итого:		26	81	-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

-визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);

-работа в малых группах (практические занятия);

- разбор практических ситуаций (практические занятия);

- работа на компьютерах(лабораторные занятия);

- метод проектов (практические занятия).

6. Тематика курсовых работ/проектов

Курсовая работа/проект не предусмотрены.

7. Контрольные работы (заочная форма обучения)

7.1. Методические указания для выполнения контрольных работ.

Цель контрольной работы - закрепление у обучающихся теоретических знаний в области защиты информации, приобретение практических навыков выбора современных средств и методов защиты информации, а также использования методов поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.

Выполнение контрольной работы обучающийся должен начинать с изучения задания, методических указаний к ее выполнению и курса лекционных и лабораторных занятий. По требованию руководителя следует собрать и изучить рекомендуемую литературу, выполнить решение представленных в методических указаниях заданий по вариантам.

Работа выполняется в обычной на листах формата А4 шрифтом №14, с соблюдением полей: сверху и снизу – 20 мм; слева – 25 мм; справа – 15 мм.

В работе необходимо представить текст задачи, решение с расчетными формулами, с объяснением буквенных обозначений, подстановкой численных значений в целых, дольных или кратных единицах системы Si (метр, Паскаль, секунда и т.д.). Окончательный результат записывается с учетом правила округления.

Решение заданий, требующих графического решения, выполняется с помощью среды имитации или графического редактора. В конце работы необходимо указать список использованных источников (в тексте обязательна ссылка на литературу).

Номера заданий соответствуют номеру варианта, который соответствует порядковому номеру обучающегося в списке группы.

К контрольной работе предъявляются следующие требования:

– контрольная работа должна быть написана на хорошем теоретическом уровне с использованием основных фундаментальных трудов по избранной теме и привлечением соответствующих фактологических материалов, статистических данных, нормативных и инструктивных документов;

– контрольная работа должна представлять самостоятельно выполненный проект, содержать критический взгляд автора на изучаемые литературные источники и практику деятельности российских и зарубежных компаний в сфере процессного управления; прикладная часть работы должна носить конкретный характер, содержать фактические данные, сравнительный анализ, расчеты;

– отдельные разделы, а также работа в целом должны заканчиваться выводами и рекомендациями для проекта, который рассматривался в практической части курсовой;

– теоретический материал и фактические данные, почерпнутые из источников, должны быть творчески переработаны, увязаны с избранной обучающимся темой и изложены авторским языком;

– работа должна быть написана четко, грамотно, научным стилем изложения и правильно оформлена: должен быть титульный лист, оглавление, страницы должны быть пронумерованы, в конце работы следует указать список источников.

Общие требования к контрольной работе:

a) четкость и логическая последовательность изложения материала;
b) убедительность аргументации;
c) краткость и точность формулировок;
d) конкретность изложения результатов работы;
e) обоснованность рекомендаций и предложений.

Титульный лист является первой страницей и служит источником информации, необходимой для определения принадлежности и поиска документа.

На титульном листе приводят следующие сведения:

a) наименование вышестоящей организации, в порядке от министерства до института;
b) наименование кафедры;
c) грифы согласования;
d) наименование темы контрольной работы;
e) должности, ученые степени, фамилии и инициалы руководителя, разработчика.

Титульный лист включают в общую нумерацию страниц отчета. Номер страницы на титульном листе не проставляют

Структурный элемент контрольной работы «ВВЕДЕНИЕ» отражает актуальность темы, объект и предмет исследования, цель и задачи исследования, методы исследования, методологические основы исследования.

«ВВЕДЕНИЕ» не должно содержать рисунков, формул, таблиц.

Во введении не рекомендуется делать обзор исторического развития проблемы и ссылаться на источники. Примерный объем введения - 2-4 листа.

Основная часть, как правило, состоит из разделов (глав), с выделением в каждом подразделов (параграфов).

Содержание разделов (глав) основной части должно точно соответствовать теме работы и полностью ее раскрывать.

Основная часть содержит:

a) анализ истории вопроса и его современного состояния, обзор литературы по исследуемой проблеме, представление различных точек зрения и обоснование позиций автора исследования, анализ и классификацию привлекаемого материала на базе избранной методики исследования;

b) описание процесса теоретических и (или) экспериментальных исследований, методов исследований, методов расчета, обоснование необходимости проведения экспериментальных работ, принципов действия разработанных объектов, их характеристики;

c) обобщение результатов исследований, включающее оценку полноты решения поставленной задачи и предложения по дальнейшим направлениям работ, оценку достоверности полученных результатов и их сравнение с аналогичными результатами отечественных и зарубежных работ.

В структурном элементе контрольной работы «ЗАКЛЮЧЕНИЕ» формулируются обобщенные выводы и предложения по результатам решения поставленных задач, указываются перспективы применения результатов на практике и возможности дальнейшего исследования проблемы, отражают оценку технико-экономической эффективности внедрения. Если определение технико-экономической эффективности невозможно, необходимо указать научную, экологическую или иную значимость работы.

Заключение не должно содержать рисунков, формул и таблиц.

Список использованной литературы и других источников составляется в следующей последовательности:

1. Законы, постановления правительства Российской Федерации и Государственной Думы.
2. Законы и постановления органов власти субъектов Российской Федерации.
3. Нормативные акты, инструктивные материалы, официальные справочники.
4. Монографическая и учебная литература в алфавитном порядке по фамилиям авторов или названиям, если на титульном листе книги автор не указан (коллективные монографии, отчеты).
5. Периодические издания с указанием года и месяца выпуска журналов и газет (если статьи из них не приведены в предыдущем разделе списка литературы).
6. Источники сети Internet.

Материал в контрольной работе располагается в следующей последовательности:

1. Титульный лист (заполняется по единой форме, его форма приведена в приложении).
2. Задание на контрольную работу.
3. Содержание.
4. Текстовое изложение контрольной работы (по главам и параграфам).
5. Список использованной литературы и источников.
6. Практический материал, использованный в работе (в виде приложения, если он не помещен по ходу изложения).

Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 3 см слева и 1,5 см – справа, 2 см – сверху и снизу.

Все листы курсовой работы должны быть пронумерованы. Каждый параграф в тексте должен иметь заголовок в точном соответствии с наименованием в плане - оглавлении.

Новый параграф можно начинать на той же странице, на которой кончился предыдущий, если на этой странице кроме заголовка поместится несколько строк текста.

Цифровые данные в сгруппированном и систематизированном виде представляются в таблицах и графиках, при этом немаловажное значение имеет оформление последних. Таблицы обычно помещаются по ходу изложения, после ссылки на них, однако не рекомендуется переносить таблицы с одной страницы на другую. Недопустимо разрывать заголовок с

таблицей, помещая их на разных страницах. Таблицы должны иметь порядковый номер, заголовок, отражающий их содержание, и примечание - ссылку на источник.

Количество цифрового материала должно соответствовать содержанию курсовой работы, не следует приводить данных, не имеющих прямого отношение к излагаемому вопросу.

В таблицах и в тексте следует избегать полного написания больших чисел. Для этого целесообразно укрупнять единицы измерения.

В работе можно использовать только общепринятые сокращения и условные обозначения.

Использованные в работе цифровые данные, выводы, высказывания других авторов в пересказе и цитаты в обязательном порядке должны сопровождаться ссылками на использованные работы. Эти ссылки могут быть сделаны в виде сносок в нижней части страницы с указанием автора, названия работы, издательства, года издания и номера страницы, где находится данное высказывание, или с указанием в скобках сразу же после высказывания номера источника в списке литературы, если речь идет о содержании всего источника. Если дается цитата, то в скобках приводятся как номер источника, так и номер страницы или страниц.

Пересказ мыслей и выводов других авторов следует делать без искажения этих мыслей, цитаты должны быть тщательно выверены и заключены в кавычки. Обучающийся несет ответственность за точность приводимых данных, а также за объективность изложения мыслей других авторов.

7.2.Тематика контрольных работ.

1. Теоретические и концептуальные основы защиты информации. Принципы защиты информации. Цели и значение защиты информации.
1. Задачи защиты информации и функции по их реализации. Виды, методы и средства защиты информации. Кадровое и ресурсное обеспечение защиты информации.
2. Источники дестабилизирующего воздействия на информацию. Понятие утечки информации, виды и причины утечки информации. Каналы утечки информации ограниченного доступа.
3. Аналитическая работа по предотвращению утраты и утечки информации. Современные подходы к понятию угрозы защищаемой информации. Объекты защиты информации.
4. Структура системы защиты информации, назначение составных частей системы. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации. Состав и классификация носителей защищаемой информации.
5. Понятие и назначение технологического обеспечения защиты информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.
6. Полномочия руководства предприятия в области защиты информации. Полномочия специальных комиссий по защите информации. Полномочия пользователей защищаемой информации.
7. Сущность и значение комплексной системы защиты информации как формы организации деятельности по защите информации.
8. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации. Собственники и владельцы информации, отнесенной к служебной и профессиональной тайне.
9. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне. Правовые и организационные принципы отнесения информации к защищаемой.
10. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.

11. Способы совершения компьютерных преступлений.
12. Модели безопасного подключения к Интернет.
13. Организация противодействия вредоносным программам.
14. Компьютерные преступления.
15. Кардерство, как вид компьютерных преступлений.
16. Государственные органы управления в области информационной безопасности, их права и обязанности.
17. Понятие «информационная война», виды и средства, применяемые в информационной войне.
18. Основные понятия классической криптографии. Требования к криптосистемам.
19. Современные криптографические алгоритмы шифрования. Подписание документов при помощи криптосистем с открытым ключом.
20. Идентификация и аутентификация электронных документов.
21. Понятие стеганографии. Применение основных методов стеганографии в процессе передачи информации.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Выполнение и защита лабораторных работ.	10
2.	Выполнение и защита практических заданий.	20
	ИТОГО за первую текущую аттестацию	30
2 текущая аттестация		
3.	Выполнение и защита лабораторных работ.	10
2.	Выполнение и защита практических заданий.	20
4.	Выполнение тестового задания.	40
	ИТОГО за вторую текущую аттестацию	70
	ВСЕГО	**100**

8.3. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся заочной формы обучения представлена в таблице 8.2.

Таблица 8.2

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1.	Выполнение и защита практических заданий	0-20
2.	Выполнение и защита лабораторных работ	0-20
3.	Выполнение контрольной работы	0-20
4.	Выполнение тестового задания	0-40
	ИТОГО текущую аттестацию	100

9. Учебно-методическое и информационное обеспечение дисциплины/модуля

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru
- Электронно-библиотечная система «Лань» https://e.lanbook.com
- Образовательная платформа ЮРАЙТ www.urait.ru
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru
- Национальная электронная библиотека (НЭБ)
- Библиотеки нефтяных вузов России :
- Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/,
- - Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/ ,
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books
- Электронная справочная система нормативно-технической документации «Технорматив»
- ЭКБСОН- информационная система доступа к электронным каталогам библиотек сферы образования и науки

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства: Windows 7 Pro x32/x64, Windows 8.1 Pro x32/x64, MS Office 2007 Pro x32/x64, MS OfficePro 2010 Pro x32/x64, MS OfficePro 2013 Pro x32/x64, MS OfficePro 2016 Pro x32/x64, FineReader 11 ProfessionalEdition, AutodeskAutoCAd 2014 x32/x64, SCADA TraceMode 6.04, MS VisualStudo 2010 x32/x64, MS VisualStudo 2013 x32/x64, 1С.Предприятие 8.2 версия для ВУЗов, MS Project 2010 x32/x64, ProjectExpert 6, БИЗНЕС-КУРС: Корпорация Плюс. Версия 4, MaplnfpPro, «Лань», PostgreSQL

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно- наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4

1	Защита информации	Лекционные занятия, практические занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Учебная мебель: столы, стулья, доска аудиторная. Моноблок - 1 шт., проектор - 1 шт., акустическая система (колонки) - 4 шт., проекционный экран - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70
		Практические занятия: Учебная аудитория для проведения занятий семинарского типа (практические занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, Оснащенность: Учебная мебель: столы, стулья, доска аудиторная. Моноблок – 1 шт., , проектор-1 шт., , акустическая система (колонки) – 4 шт., проекционный экран – 1 шт., документ-камера – 1 шт., телевизор – 2 шт.	625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70
		Лабораторные занятия: Учебная аудитория для проведения занятий семинарского типа (лабораторные работы); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, Учебная мебель: столы, стулья, доска аудиторная. Учебно-лабораторные комплексы "Локальные вычислительные сети": «Сетевая безопасность» (1 шт.), «Корпоративные компьютерные сети» (1 шт.); Компьютер в комплекте (7 шт.).	625027, Тюменская область, г. Тюмень, ул. 50 лет Октября, д. 38

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям.

Систематическое и аккуратное выполнение всей совокупности лабораторных работ позволит обучающемуся в выполнении лабораторных работ, а также облегчить работу преподавателя по организации овладениями умением самостоятельно проводить лабораторные работы, фиксировать результаты, анализировать их, делать выводы в целях дальнейшего использования полученных знаний и умений.

Целями выполнения лабораторных работ является:

- обобщение, систематизация, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике;
- реализация единства интеллектуальной и практической деятельности;
- развитие необходимых компетенций у обучаемых.

Общие требования. Для более эффективного выполнения лабораторных работ необходимо повторить соответствующий теоретический материал, а на занятиях, прежде всего, внимательно ознакомиться с содержанием работы и оборудованием. В ходе работы необходимо строго соблюдать правила по технике безопасности.

Письменные инструкции к каждой лабораторной работе, приведены в комплекте заданий к лабораторным работам.

Весь процесс выполнения лабораторных работ включает в себя:

- теоретическую подготовку;
- ознакомление с заданием;
- проведение лабораторной работы;
- оформление и обработка результатов лабораторно эксперимента;

– защита отчета по выполненной работе.

11.2. Методические указания по организации самостоятельной работы.

СРС – важнейшая составная часть учебного процесса, обязательная для каждого обучающегося, объем которой определяется учебным планом. Методологическую основу СРС составляет деятельностный подход, при котором цели обучения ориентированы на формирование умений решать типовые и нетиповые задачи, т. е. на реальные ситуации, в которых обучающимся надо проявить знание конкретной дисциплины.

Предметно и содержательно СРС определяется государственным образовательным стандартом, действующими учебными планами по образовательным программам очной и заочной форм обучения, рабочими программами учебных дисциплин, средствами обеспечения СРС: учебниками, учебными пособиями и методическими руководствами, учебно-программными комплексами и т.д.

Планируемые результаты грамотно организованной СРС предполагают:

- усвоение знаний, формирование профессиональных умений, навыков и компетенций будущего специалиста; закрепление знания теоретического материала практическим путем;
- воспитание потребности в самообразовании;
- максимальное развитие познавательных и творческих способностей личности;
- побуждение к научно-исследовательской работе;
- повышение качества и интенсификации образовательного процесса; формирование интереса к избранной профессии и овладению ее особенностями;
- осуществление дифференцированного подхода в обучении;
- применение полученных знаний и практических навыков для анализа ситуации и выработки правильного решения, для формирования собственной позиции, теории, модели.

Достижение планируемых результатов позволит придать инновационный характер современному образованию, а, следовательно, решить задачи его модернизации.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Защита информации
Код, направление подготовки: 09.03.01.,Информатика и вычислительная техника
Направленность (профиль): Автоматизированные системы обработки и управления информации

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения	Критерии оценивания результатов обучения			
			1-2	3	4	5
ОПК-1	ОПК-1.1. Обладает фундаментальными знаниями, полученными при изучении математических, естественнонаучных и общеинженерных дисциплин, методами теоретического и экспериментального исследования и применяет их при решении стандартных задач профессиональной деятельности.	Знать: З1 – фундаментальные основы из области естественнонаучных и общеинженерных дисциплин, относящиеся к защите информации..	Не знает основы защиты информации в информационных системах и сетях.	Частично знает методы защиты информации в информационных системах и сетях.	Демонстрирует достаточные знания основ защиты информации в информационных системах и сетях.	Демонстрирует исчерпывающие знания основ защиты информации в информационных системах и сетях.
		Уметь: У1–применять фундаментальные знания из области естественнонаучных и общеинженерных дисциплин при защите автоматизированных систем.	Не умеет решать стандартные задачи защиты информации в информационных системах и сетях	Демонстрирует отдельные навыки применения стандартных задач защиты информации в информационных системах и сетях	Демонстрирует достаточные навыки умения применять стандартные задачи защиты информации в информационных системах и сетях	Демонстрирует исчерпывающие навыки умения стандартные задачи защиты информации в информационных системах и сетях
		Владеть:В1-методами теоретического и экспериментального исследования защищенности автоматизированных систем.	Не владеет методами теоретического и экспериментального исследования защиты автоматизированных систем	Владеет методами теоретического и экспериментального исследования защиты автоматизированных систем	В достаточном объёме владеет методами теоретического и экспериментального исследования защиты автоматизированных систем	В полном объёме владеет методами теоретического и экспериментального исследования защиты автоматизированных систем
ОПК-2	ОПК-2.1. Обладает знаниями современных информационных технологий и	Знать: З2 - современные информационные технологии и	Не знает современные технологии и методы защиты в информационных	Частично знает современные технологии и методы защиты в	Знает современные технологии и методы защиты в информационных	В полном объёме знает современные технологии и методы защиты в

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения	Критерии оценивания результатов обучения			
			1-2	3	4	5
	программных средств, методов их использования, демонстрирует навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	программные средства в области защиты информационных систем.	системах и сетях	информационных системах и сетях	системах и сетях	информационных системах и сетях
		Уметь: У2 – использовать современные информационные технологии и программные средства, в том числе отечественного производства, в области защиты информации.	Не умеет выбирать современные технологии и методы защиты в информационных системах и сетях	Частично умеет выбирать современные технологии и методы защиты в информационных системах и сетях	Умеет выбирать современные технологии и методы защиты в информационных системах и сетях	В полном объёме умеет выбирать современные технологии и методы защиты в информационных системах и сетях
		Владеть: В2 - навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, в области защиты информации.	Не владеет способами применения современных технологий и средств защиты в информационных системах и сетях.	Демонстрирует отдельные навыки применения современных технологий и средств защиты в информационных системах и сетях	Демонстрирует достаточные познания современных технологий и средств защиты в информационных системах и сетях	В полном объёме демонстрирует познания применения современных технологий и средств защиты в информационных системах и сетях
ОПК-3	ОПК-3.1. Демонстрирует знание принципов информационной и библиографической культуры, способность применять методы поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций,	Знать: З3 – принципы информационной и библиографической культуры в области защиты информации.	Не знает методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.	Знает частично методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.	Знает методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.	В полном объёме знает методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.
		Уметь: У3 - применять методы поиска и	Не умеет решать стандартные задачи	Частично умеет решать стандартные	Умеет решать стандартные задачи	В полном объёме умеет решать стандартные

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения	Критерии оценивания результатов обучения			
			1-2	3	4	5
	применяет методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций.	информационной безопасности операционных систем, баз данных и сетей	задачи информационной безопасности операционных систем, баз данных и сетей	информационной безопасности операционных систем, баз данных и сетей	задачи информационной безопасности операционных систем, баз данных и сетей
		Владеть: В3 - методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	Не владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.	Частично владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.	Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.	В полном объёме владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.

Приложение 2

КАРТА

обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина: **Защита информации**
Код, направление подготовки:**09.03.01. Информатика и вычислительная техника**
Направленность (профиль): **Автоматизированные системы обработки информации и управления**

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Лось А.Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд. - Москва : Юрайт, 2023. - 473 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-534-12474-3 : 1089.00 р. - Текст : непосредственный. Режим доступа: https://urait.ru/bcode/511138	ЭР	30	100	+
2	Пилиди В. С. Математические основы защиты информации : учебное пособие / В. С. Пилиди. - Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ЭБС "IPR BOOKS". - ISBN 978-5-9275-3363-3 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/95786.html	ЭР	30	100	+
3	Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров. - Издание 2-е, стереотипное. - [Б. м.] : Горячая линия-Телеком, 2016. - 304 с. - ЭБС Лань. - **ISBN** 978-5-9912-0439-2 : ~Б. ц. - Текст : непосредственный. Режим доступа: https://e.lanbook.com/book/111005	ЭР	30	100	+
4	Фомичёв В. М. Криптографические методы защиты информации : учебник для вузов : в 2 ч. Ч. 1. Математические аспекты / В. М. Фомичёв, Д. А. Мельников. - Москва : Юрайт, 2022. - 209 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-9916-7088-3 : 539.00 р. - Текст : непосредственный. Режим доступа: https://urait.ru/bcode/489745	ЭР	30	100	+
5	Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2023. - 349 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-534-02883-6 : 829.00 р. - Текст : непосредственный. Режим доступа: https://urait.ru/bcode/511890	ЭР	30	100	+
6	Костин В. Н. Методы и средства защиты компьютерной информации:	ЭР	30	100	+

	аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. - Москва : Издательский Дом МИСиС, 2018. - 21 с. - ЭБС "IPR BOOKS". - ISBN 978-5-906953-22-3 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/98199.html				
7	Костин В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. - Москва : Издательский Дом МИСиС, 2018. - 31 с. - ЭБС "IPR BOOKS". - ISBN 978-5-906953-53-7 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/98200.html	ЭР	30	100	+
8	Костин В. Н. Методы и средства защиты компьютерной информации: криптографические методы для защиты информации : учебное пособие / В. Н. Костин. - Москва : Издательский Дом МИСиС, 2018. - 40 с. - ЭБС "IPR BOOKS". - ISBN 978-5-90695-334-6 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/98201.html	ЭР	30	100	+
9	Никифоров С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2022. - 160 с. - ЭБС Лань. - ISBN 978-5-8114-4042-9 : ~Б. ц. - Текст : непосредственный Режим доступа: https://e.lanbook.com/book/206285	ЭР	30	100	+
10	Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 124 с. - ЭБС Лань. - ISBN 978-5-8114-9563-4 : ~Б. ц. - Текст : непосредственный. Режим доступа: https://e.lanbook.com/book/200483	ЭР	30	100	+
11	Нестеров С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2022. - 324 с. - ЭБС Лань. - ISBN 978-5-8114-4067-2 : ~Б. ц. - Текст : непосредственный. Режим доступа: https://e.lanbook.com/book/206279	ЭР	30	100	+
12	Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - Саратов : Профобразование, 2019. - 702 с. - ЭБС "IPR BOOKS". - ISBN 978-5-4488-0070-2 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/87995.html	ЭР	30	100	+
13	Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - Саратов : Профобразование, 2019. - 543 с. - ЭБС "IPR BOOKS". - ISBN 978-5-4488-0074-0 : ~Б. ц. - Текст : непосредственный. Режим доступа:	ЭР	30	100	+

	http://www.iprbookshop.ru/87992.html				
14	Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л. Е. Бахаров. - Москва : Издательский Дом МИСиС, 2019. - 59 с. - ЭБС "IPR BOOKS". - ISBN 978-5-906953-94-0 : ~Б. ц. - Текст : непосредственный. Режим доступа: http://www.iprbookshop.ru/98171.html	ЭР	30	100	+
15	Никифоров С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 96 с. - ЭБС "Лань". - ISBN 978-5-8114-9562-7 : ~Б. ц. - Текст : непосредственный. Режим доступа: https://e.lanbook.com/book/200480	ЭР	30	100	+

*ЭР – электронный ресурс доступный через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/