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

УТВЕРЖДАЮ

Председатель КСН
О.Н. Кузяков

«06» 07 2019 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 в соответствии с утвержденным учебным планом от 22. 04.2019 г. и требованиями ОПОП по направлению 09.03.01, Информатика и вычислительная техника,направленность (профиль) Автоматизированные системы обработки информации и управления,к результатам освоения дисциплины «Защита информации».

Рабочая программа рассмотрена
на заседании кафедры кибернетических систем

Протокол № _16__ от «_6_» ____07_____ 2019г.

Заведующий кафедрой _____ О.Н. Кузяков

СОГЛАСОВАНО:
Заведующий выпускающей кафедро
кибернетических систем _____ О.Н. Кузяков

«6_» ___07_____ 2019 г.

Рабочую программу разработал:

Б.В. Семенов, доцент кафедры КС, к.т.н. _____

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.

Необходимыми условиями для освоения дисциплины являются:

Знание: структур и принципов организации операционных систем; основы администрирования вычислительных сетей; основы управления базами данных; эталонную модель взаимодействия открытых систем.

Умения: применять методы настройки операционных систем, вычислительных сетей и баз данных.

Владение: стандартными методами и средствами защиты информации в компьютерных системах и сетях.

Содержание дисциплины является логическим продолжением содержания дисциплин: «Правовое обеспечение информационных технологий», «Информатика», «Программирование», «Операционные системы», «Системы искусственного интеллекта» и служит основой для освоения дисциплин: «Методы оптимизации и теория принятия решений», «Основы научных исследований в области информационных систем и технологий», «Проектирование автоматизированных информационных систем», «Корпоративные сети», а также может быть использовано при выполнении курсовых работ и ВКР.

3. Результатыобучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)[1]	Код и наименование результата обучения по дисциплине (модулю)
ОПК-1. Способен	**Знать:**	Знать: З1 -основы

применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.З1-основы высшей математики, физики, экологии, инженерной графики, информатики и программирования.	защиты информации в информационных системах и сетях
	Уметь: ОПК-1.У1. решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, вычислительных методов.	Уметь:У1–решать стандартные задачи защиты информации в информационных системах и сетях
	Владеть: ОПК-1.В1. методами теоретического и экспериментального исследования инженерных задач.	Владеть:В1-методами теоретического и экспериментального исследования защиты автоматизированных систем
ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	**Знать:** ОПК-2.З2-современные информационные технологии и методы их использования при решении задач профессиональной деятельности.	Знать: З2 - современные технологии и методы защиты в информационных системах и сетях
	Уметь: ОПК-2.У2-выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.	Уметь: У2 - выбирать современные технологии и методы защиты в информационных системах и сетях.
	Владеть: ОПК-2.В2-способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Владеть: В2 - способами применения современных технологий и средств защиты в информационных системах и сетях.
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с	**Знать:** ОПК-3.З4. методы и средства решения стандартных задач профессиональной деятельности с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать: З3 - методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.
	Уметь: ОПК-3.У3. решать стандартные задачи профессиональной деятельности	Уметь: У3 - решать стандартные задачи информационной безопасности операционных систем, баз

учетом основных требований информационной безопасности	на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	данных и сетей
	Владеть: ОПК-3.В3. методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	Владеть: В3 - методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе требований информационной безопасности.

4. Объем дисциплины «Защита информации»

Общий объем дисциплины составляет 4 зачетных единиц, 144 часа.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
очная	4/7	30	15	15	84	зачёт
заочная	4/8	8	4	8	124	зачёт

5. Структура и содержание дисциплины/модуля

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 [2]
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в курс. Источники, риски и формы атак на информацию.	2	2	2	5	11	ОПК-1.З1 ОПК-1.У1 ОПК-1.В1 ОПК-2.З2 ОПК-2.У2	Опрос,собеседование,КР,Отчёты

2	2	Источники, риски и формы атак на информацию	6	2	2	10	20	ОПК-2.В2 ОПК-3.З3 ОПК-3.У3 ОПК-3.В3	Опрос, собеседование, КР, Отчёты
3	3	Криптографические модели, алгоритмы шифрования.	4	3	3	14	26		Опрос,собеседование,КР, Отчёты
4	4	Политика безопасности, стандарты безопасности.	4	2	2	10	18		Опрос,собеседование,КР, Отчёты
5	5	Защита данных в операционных системах	6	3	3	8	20		Опрос,собеседование,КР, Отчёты
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях.	8	3	3	10	24		Опрос,собеседование,КР, Отчёты
7	Зачет		-	-	-	27	27		
Итого:			30	15	15	84	144		

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. Источники, риски и формы атак на информацию.	1		1	7	9	ОПК-1.З1 ОПК-1.У1 ОПК-1.В1 ОПК-2.З2 ОПК-2.У2 ОПК-2.В2 ОПК-3.З3 ОПК-3.У3 ОПК-3.В3	Опрос,собеседование,КР, Отчёты
2	2	Источники, риски и формы атак на информацию	1	1	1	16	19		Опрос,собеседование,КР, Отчёты
3	3	Криптографические модели, алгоритмы шифрования.	1	1	2	16	18		Опрос,собеседование,КР ,Отчёты
4	4	Политика безопасности, стандарты безопасности.	1	1	1	16	19		Опрос,собеседование,КР, Отчёты
5	5	Защита данных в операционных системах	2	1	1	21	25		Опрос,собеседование,КР, Отчёты
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях.	2		2	15	16		Опрос,собеседование,КР, Отчёты
7	Зачет		-	-	-	27	27		
Итого:			8	4	8	124	144		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

№	Наименование раздела	Дидактическая единица

раздела		
1	Введение в курс. Источники, риски и формы атак на информацию.	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.
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
3	Криптографические модели, алгоритмы шифрования.	Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.
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. Руководящие документы Гостехкомиссии России по защите от НСД к информации.
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.
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	Тема лекции		
		ОФО	ЗФО	
1	1	2	1	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.
2	2	6	1	Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС
3	3	4	1	Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.
4	4	4	1	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. Руководящие документы Гостехкомиссии России по защите от НСД к информации.
5	5	6	2	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.
6	6			Многоуровневая зашита корпоративных сетей. Сетевые протоколы

		8	2	защиты информации. Сканирование и мониторинг информационной безопасности.
Итого:		30	8	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Тема практического занятия		
		ОФО	ЗФО	
1	1	2		Основные понятия и определения.
2	2	2	1	Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы.
3	3	3	1	Криптографические системы и протоколы.
4	5	2	1	Классы и группы защищенности средств вычислительной техники и АС от НСД и требования к ним. Руководящие документы Гостехкомиссии России по защите от НСД к информации.
5	5	3	1	Модели безопасности и типовая архитектура подсистемы защиты операционной системы, основные функции. Основные компоненты системы безопасности ОС на примере семейств ОС Windows / Unix.
6	6	3		Многоуровневая зашита корпоративных сетей. Сетевые протоколы защиты информации.
Итого:		15	4	

Лабораторные работы

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Наименование лабораторной работы		
		ОФО	ЗФО	
1	1	2	1	Лабораторная работа № 1. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации
2	2	2	1	Лабораторная работа №2. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей
3	3	3	2	Лабораторная работа №3.Разработка и программная реализация криптографических алгоритмов
4	4	2	1	Лабораторная работа №4. Использование функций криптографического интерфейса Windows для защиты информации
5	5	3	1	Лабораторная работа №5. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ
6	6	3	2	Лабораторная работа №6. Защита программного обеспечения от несанкционированного использования и копирования
Итого:		15	8	

Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины	Тема			Вид СРС
		ОФО	ЗФО		
1	1	5	7	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
2	2	10	16	Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
3	3.	14	16	Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
4	4.	10	16	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. Руководящие документы Гостехкомиссии России по защите от НСД к информации.	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
5	5	8	21	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.	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
6	6	10	15	Многоуровневая зашита корпоративных сетей. Сетевые протоколы защиты информации. Сканирование и мониторинг информационной безопасности.	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
7	Зачет	27	27		Изучение пройденного материала. Подготовка к зачету
Итого:		84	124		

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 не предусмотрено.

7. Контрольные работы

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.

7.2. Задания для контрольных работ представлены в методических рекомендациях:

Семенов Б.В., Защита информации [Текст] : методические рекомендации по выполнению контрольных работ обучающимися заочной формы обучения по направлениям 09.03.01 «Информатика и вычислительная техника» / Тюмень : ТюмГНГУ, 2016. - 22 с.

8. Оценка результатов освоения дисциплины/модуля

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 лабораторных работ	12
2	Защита лабораторных работ	4
3	Самостоятельная работа	10
4	Практические занятия	5
	ИТОГО за первую текущую аттестацию	31
2 текущая аттестация		
1	Выполнение лабораторных работ	12
2	Защита лабораторных работ	4
3	Самостоятельная работа	10
4	Практические занятия	5
	ИТОГО за вторую текущую аттестацию	31
2 текущая аттестация		
1	Выполнение лабораторных работ	18
2	Защита лабораторных работ	6
3	Самостоятельная работа	10
4	Теоретический контроль	4
	ИТОГО за третью текущую аттестацию	38
	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	Работа на практических занятиях	0-4
2	Выполнение практической работы	0-20
3	Выполнение контрольных работы	0-10
4	Выполнение лабораторных работ	0-40
5	Защита лабораторных работ	0-16
6	Опрос теоретического материала	0-10
	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:

- zbMATH(zbMATH.com) – самая полная математическая база данных;
- exponent.ru
- ЭБС «Издательства Лань»;
- ЭБС «Электронного издательства ЮРАЙТ»;
- Собственная полнотекстовая база (ПБД) БИК ТИУ;
- Научная электронная библиотека «eLIBRARY.RU»;
- ЭБС «IPRbooks»;
- Научно-техническая библиотека ФГБОУ ВО РГУ нефти и газа имени И.М. Губкина;
- Научно-техническая библиотека ФГБОУ ВПО УГНТУ (г. Уфа);
- Научно-техническая библиотека ФГБОУ ВПО УГТУ (г. Ухта);
- ЭБС «Проспект»;
- ЭБС «Консультант студент».

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

1. Microsoft Office Professional Plus;

2. Windows 8.

3.Маткад.

4. Матлаб и FuzzyTech.

10. Материально-техническое обеспечение дисциплины/модуля

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

Таблица 10.1

№ п/п	Перечень оборудования, необходимого для освоения дисциплины/модуля	Перечень технических средств обучения, необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
1	625039, г. Тюмень, ул. Мельникайте, д. 70. Учебная аудитория для проведения занятий лекционного и семинарского типа (практические занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации.	**Оснащенность:** Учебная мебель: столы, стулья. Моноблок - 1 шт.; проектор- 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., документ- камера - 1 шт., телевизор - 2 шт., микрофон - 1 шт. **Программное обеспечение:** Microsoft Windows (Договор №5378-19 от 02.09.2019 до 01.09.2020), Microsoft Office Professional Plus (Договор №5378-19 от 02.09.2019 до 01.09.2020).
2	625039, г. Тюмень, ул. Мельникайте, д. 70, ауд.302. Учебная аудитория для проведения занятий семинарского типа (лабораторные занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации.	**Оснащенность:** Учебная мебель: столы, стулья, столы компьютерные. Моноблок - 11 шт., проектор -1 шт., акустическая система (колонки) - 2 шт., интерактивная доска -1 шт., передвижная магнитно-маркерная доска - 1 шт.. **Программное обеспечение:** Microsoft Windows (Договор №5378-19 от 02.09.2019 до 01.09.2020), Microsoft Office Professional Plus (Договор №5378-

		19 от 02.09.2019 до 01.09.2020), в т.ч. рекомендуемое программное обеспечение для установки к моменту проведения лабораторных занятий
3	Помещение для самостоятельной работы обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.	**Оснащенность:** Учебные столы, стулья. Доска меловая. Компьютер в комплекте -5 шт. **Программное обеспечение:** Microsoft Windows (Договор №5378-19 от 02.09.2019 до 01.09.2020), Microsoft Office Professional Plus (Договор №5378-19 от 02.09.2019 до 01.09.2020)

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям. Методические указания по подготовке к практическим занятиям. На практических занятиях обучающиеся изучают методику и выполняют типовые расчеты. В процессе подготовки к практическимзанятиям обучающиеся могут прибегать к консультациям преподавателя. Наличие конспекта лекций на практическом занятии ОБЯЗАТЕЛЬНО! Задания на выполнение, на практических занятиях обучающиеся получают индивидуально. Порядок выполнения заданий изложены в следующих методических указаниях:

1. Семенов Б.В. Защита информации [Текст] : методические рекомендации к лабораторным (практическим) занятиям и самостоятельной работе для обучающихся направления 09.03.01 «Информатика и вычислительная техника» всех форм обучения / ТюмГНГУ ;С16, 2017г.

2. Семенов Б.В. Защита информации [Текст] : методические рекомендации по выполнению контрольных работ обучающимися заочной формы обучения по направлениям 09.03.01 «Информатика и вычислительная техника» / ТюмГНГУ ,С 22,2016г.

3. Семенов Б.В. Защита информации техническими средствами [Текст] : методические рекомендации к лабораторным занятиям и самостоятельной работе для магистрантов направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» программа «Автоматизация технологических процессов нефтегазодабычи» очной формы обучения / ТИУ, 26с, 2018 ;

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения. Преподаватель на занятии дает рекомендации необходимые для освоения материала. В ходе самостоятельной работы, обучающиеся должны выполнить задания на компьютере с помощью пакетов прикладных программ, изучить теоретический материал по разделам. Обучающиеся должны понимать содержание выполненной работы (знать определения понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п).

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 и наименование результата обучения по дисциплине«Защита мнформации»	Критерии оценивания результатов обучения			
		1-2	3	4	5
ОПК-1	Знать: З1 - основы защиты информации в информационных системах и сетях	Не знает основы защиты информации в информационных системах и сетях.	Частично знает методы защиты информации в информационных системах и сетях.	Демонстрирует достаточные знания основзащиты информации в информационных системах и сетях.	Демонстрирует исчерпывающие знания основзащиты информации в информационных системах и сетях.
	Уметь:У1–решать стандартные задачи защиты информации в информационных системах и сетях	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 защиты 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	Знать: З2 - современные технологии и методы защиты в информационных системах и сетях	Не знает современные технологии и методы защиты в информационных системах и сетях	Частично знает современные технологии и методы защиты в информационных системах и сетях	Знает современные технологии и методы защиты в информационных системах и сетях	В полном объёме знает современные технологии и методы защиты в информационных системах и сетях

Код компетенции	Код и наименование результата обучения по дисциплине«Защита мнформации»	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Уметь: У2 - выбирать современные технологии и методы защиты в информационных системах и сетях.	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 - способами применения современных технологий и средств защиты в информационных системах и сетях.	Не владеетспособами 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	Знать: З3 - методы и средства решения стандартных задач информационной безопасности операционных систем, баз данных и сетей.	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 - решать стандартные задачи информационной безопасности операционных систем, баз данных и сетей	Не умеет решать стандартные задачи информационной безопасности операционных систем, баз данных и сетей	Частично умеет решать стандартные задачи информационной безопасности операционных систем, баз данных и сетей	Умеет решать стандартные задачи информационной безопасности операционных систем, баз данных и сетей	В полном объёме умеет решать стандартные задачи информационной безопасности операционных систем, баз данных и сетей

Код компетенции	Код и наименование результата обучения по дисциплине«Защита мнформации»	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: В3 - методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций на основе 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	Названиеучебного,учебно-методическогоиздания, автор,издательство, вид издания, год издания	Количество экземпляров вБИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта ЭБС (+/-)
1	**Рябко, Б.Я.** Криптографические методы защиты информации : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2012. — 229 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/5193	ЭР	20	100	ЭБС Лань
2	**Романьков, В. А.** Введение в криптографию [Текст] : курс лекций : студентам вузов / В. А. Романьков. - 2-е изд., испр. и доп. - Москва : ФОРУМ, 2012. - 239 с.	15	20	100	-

3	**Мельников, В.П. Методы и средства хранения и защиты компьютерной информации** [Текст]: учебник для студентов вузов, обучающихся по направлениям: "Автоматизация технологических процессов и производств", "Конструкторско-технологическое обеспечение машиностроительных производств" / В. П. Мельников, А. Г. Схиртладзе ; ред. В. П. Мельников. - Старый Оскол : ТНТ, 2014. - 399 с	15	20	100	-

Заведующий кафедрой
кибернетических систем О.Н. Кузяков

«6» 07 2019 г.

Директор БИК Д.Х. Каюкова

«6» 07 2019 г.

М.П.

Дополнения и изменения
к рабочей программе по дисциплине
«Защита информации»
на 2019-2020 учебный год

В рабочую программу дисциплины вносятся следующие дополнения:

в материально-техническое обеспечение дисциплины включить программное обеспечение, необходимое для успешного освоения образовательной программы: Zoom (бесплатная версия), свободно-распространяемое ПО

Дополнения и изменения внес
К.т.н., доцент _____С.М. Каратун

Дополнения (изменения) в рабочую программу дисциплины рассмотрены и одобрены на заседании кафедры кибернетических систем.

Протокол от «_19_» _____04_____ 2020г. №____8_____

Заведующий кафедрой
Кибернетических систем _____ О.Н. Кузяков

СОГЛАСОВАНО:
Зав. выпускающей кафедрой
кибернетических систем _____О.Н. Кузяков

«_19__» _____04_____ 2020г.

Дополнения и изменения
к рабочей программе по дисциплине
«Защита информации»
на 2020-2021 учебный год

В рабочую программу дисциплины вносятся следующие дополнения (изменения):

в материально-техническое обеспечение дисциплины включить следующий перечень лицензионного программного обеспечения, необходимого для успешного освоения образовательной программы: Microsoft Office Professional Plus, Договор №6714-20 от 31.08.2020 до 31.08.2021; Microsoft Windows, Договор №6714- 20 от 31.08.2020 до 31.08.2021; Zoom (бесплатная версия), Свободно-распространяемое ПО

Дополнения и изменения внес
К.т.н., доцент _____С.М. Каратун

Дополнения (изменения) в рабочую программу дисциплины рассмотрены и одобрены на заседании кафедры кибернетических систем.

Протокол от «_1_» _____09_____ 2020г. №____1_____

Заведующий кафедрой
Кибернетических систем _____ О.Н. Кузяков

СОГЛАСОВАНО:
Зав. выпускающей кафедрой
кибернетических систем _____О.Н. Кузяков

«_01__» _____09_____ 2020г.

Дополнения и изменения
к рабочей программе по дисциплине
«Защита информации»
на 2021-2022 учебный год

На основании изменений, внесенных в ФГОС ВО приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1456 (зарегистрирован Министерством юстиции Российской федерации 27 мая 2021 г. регистрационный номер №63650), в рабочую программу дисциплины вносятся следующие дополнения (изменения):

компетенцию ОПК-2 изложить в следующей редакции:
«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».

Дополнения и изменения внес
К.т.н., доцент _____С.М. Каратун

Дополнения (изменения) в рабочую программу дисциплины рассмотрены и одобрены на заседании кафедры кибернетических систем.
Протокол от «_30_» _____08_____ 2021г. №____1_____

Заведующий кафедрой
Кибернетических систем _____ О.Н. Кузяков

СОГЛАСОВАНО:
Зав. выпускающей кафедрой
кибернетических систем _____О.Н. Кузяков

«_30__» _____08_____ 2021г.

Дополнения и изменения
к рабочей программе дисциплины (модуля)
_____

на 20_ - 20_ учебный год

В рабочую программу вносятся следующие дополнения (изменения):
_____

_____

_____

_____

Дополнения и изменения внес:
Доцент кафедры КС, к.т.н. _____Б.В. Семенов

Дополнения (изменения) в рабочую программу рассмотрены и одобрены на заседании кафедры Кибернетических систем.

Протокол от «____» _____20__ г. № _____.

Заведующий кафедрой_____ О.Н. Кузяков.

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой/
Руководить образовательной программы _____ О.Н. Кузяков.

«_____» _____ 20___ г.