

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Клочков Юрий Сергеевич  
Должность: и.о. ректора  
Дата подписания: 29.03.2024 11:40:57  
Уникальный программный ключ:  
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
**«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»**

**УТВЕРЖДАЮ**

Председатель КСН



О.Н. Кузяков

« 1 » 09 \_\_\_\_\_ 2020 г.

**РАБОЧАЯ ПРОГРАММА**

дисциплины: Защита информации в автоматизированных информационных системах

направление подготовки: 09.04.01 Информатика и вычислительная техника

направленность (профиль): Нейросетевые технологии в автоматизированных системах управления

форма обучения: очная/ заочная

Рабочая программа разработана в соответствии с утвержденным учебным планом от 8 июня 2020 г. и требованиями ОПОП по направлению подготовки 09.04.01 Информатика и вычислительная техника, направленность (профиль): Нейросетевые технологии в автоматизированных системах управления, к результатам освоения дисциплины «Защита информации в автоматизированных информационных системах».

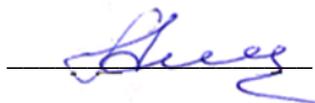
Рабочая программа рассмотрена  
на заседании кафедры КС

Протокол № 1 от «1» 09 2020 г.

Заведующий кафедрой  О.Н. Кузяков

Рабочую программу разработал:

А.М. Андриянов, доцент кафедры КС, к.т.н.



## 1. Цели и задачи освоения дисциплины

Цель дисциплины: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно - технической защиты информации;
- изучение организационных основ инженерно-технической защиты информации.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации в автоматизированных информационных системах» относится к дисциплинам обязательной части Блока 1 учебного плана.

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: «Интеллектуальные системы», «Параллельные методы и алгоритмы», «Современные численные методы, пакеты прикладных программ и нейропакеты» и служит основой для прохождения преддипломной практики и 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
УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Знать: УК-1.31- процедуры критического анализа	Знать: З1 методы анализа своих проблемных ситуаций
	Уметь: УК-1.У1 -принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий.	Уметь: У1-принимать решения при проблемных ситуациях

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
	<b>Владеть:</b> УК-1.В1- методами установления причинно-следственных связей и определения наиболее значимых среди них.	<b>Владеть:</b> В1- методами решения при проблемных ситуациях
ОПК-1 - Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	<b>Знать:</b> ОПК-1.31 - математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	<b>Знать:</b> 32- методы защиты информации в АИС.
	<b>Уметь:</b> ОПК-1.У1 - решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	<b>Уметь:</b> У2-применять методы защиты информации в АИС.
	<b>Владеть:</b> ОПК-1.В1 - методами теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте.	<b>Владеть:</b> В2- методами защиты информации в АИС.
ОПК-2 - Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач.	<b>Знать:</b> ОПК-2.32 - современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач.	<b>Знать:</b> 33- современные информационные технологии и инструментальные среды защиты информации АИС.
	<b>Уметь:</b> ОПК-2.У2 - обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач.	<b>Уметь:</b> У3- обосновывать выбор современных информационных технологий защиты информации АИС.
	<b>Владеть:</b> ОПК-2.В2 - методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, для решения профессиональных задач.	<b>Владеть:</b> В3- методами разработки программных средств защиты информации АИС.
ОПК-5 – Способен разрабатывать и модернизировать программное и аппаратное обеспечение	<b>Знать</b> ОПК-5.36 - современное программное и аппаратное обеспечение информационных и автоматизированных систем.	<b>Знать:</b> 34- современное аппаратно-программное обеспечение защиты информации в АИС

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
информационных и автоматизированных систем	<b>Уметь</b> ОПК-5.У6 - разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач.	Уметь: У4 – модернизировать аппаратно-программное обеспечение защиты информации в АИС
	<b>Владеть</b> ОПК-5.В5 - методами модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач.	Владеть: В4- методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.

#### 4. Объем дисциплины

Общий объем дисциплины составляет 4 зачетных единицы, 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	2/4	14	14	26	90	экзамен
заочная	2/4	6	4	10	124	экзамен

#### 5. Структура и содержание дисциплины

##### 5.1. Структура дисциплины.

##### очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства <sup>1</sup>
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Международные стандарты информационного обмена. Понятие угроз. Информационная безопасность в условиях функционирования в России глобальных сетей	1	1	2	5	9	УК-1 (31,У1,В1)	типовой расчет, опрос
2	2	Три вида возможных нарушений информационной системы.	2	2	4	16	24	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5	типовой расчет, опрос

<sup>1</sup>Эссе, реферат, тест, типовой расчет, опрос (устный или письменный), собеседование, РГР, контрольная работа, творческое задание, кейс-задача, деловая игра, презентация доклада, отчет и т.д.

								(36,У6,В5.)	
3	3	Основные положения теории информационной безопасности. Модели безопасности и их применение.	2	2	4	16	24	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
4	4	Анализ способов нарушений информационной безопасности.	2	2	2	14	20	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
5	5	Использование защищенных компьютерных систем.	2	2	4	5	13	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
6	6	Основные технологии построения защищенных систем.	1	1	2	2	6	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
7	7	Место информационной безопасности экономических систем в национальной безопасности страны.	4	4	8	5	21	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
8	Зачет/экзамен		-	-	-	27	27		
Итого:			14	14	26	92	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	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей	1		1	7	9	УК-1 (31,У1,В1)	типовой расчет, опрос
2	2	Три вида возможных нарушений информационной системы.	1	1	1	16	19	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
3	3	Основные положения теории информационной безопасности. Модели безопасности и их применение.	1	1	2	16	20	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
4	4	Анализ способов нарушений информационной безопасности.	1	1	2	16	20	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
5	5	Использование защищенных компьютерных систем.	1	1	2	16	20	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5	типовой расчет, опрос

								(36,У6,В5.)	
6	6	Основные технологии построения защищенных систем.				9	9	ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
7	7	Место информационной безопасности экономических систем в национальной безопасности страны.	1	2	17	20		ОПК-1 (31,У1,В1) ОПК-2 (32,У2,В2) ОПК-5 (36,У6,В5.)	типовой расчет, опрос
		Контрольная работа				18	18		
8		экзамен	-	-	-	9	9		
Итого:			6	4	10	124	144		

## 5.2. Содержание дисциплины.

### 5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей

Раздел 2. Три вида возможных нарушений информационной системы.

Раздел 3 Основные положения теории информационной безопасности. Модели безопасности и их применение.

Раздел 4 Анализ способов нарушений информационной безопасности.

Раздел 5 Использование защищенных компьютерных систем.

Раздел 6 Основные технологии построения защищенных систем.

Раздел 7 Место информационной безопасности экономических систем в национальной безопасности страны.

### 5.2.2. Содержание дисциплины по видам учебных занятий.

#### Лекционные занятия

Таблица 5.2.1

№ п/п	Ном ер разд ела дисц ипли ны	Тема лекции		
		ОФО	ЗФО	
1	1	1	1	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.
2	2	2	1	Три вида возможных нарушений информационной безопасности.

				Три составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от уроз.
3	3	2	1	Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.
4	4	2	1	Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
5	5	2	1	Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике.
6	6	1		Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.
7	7	4	1	Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.
Итого:		14	6	

### Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Тема практического занятия		
		ОФО	ЗФО	
1	1	1		Информационная безопасность
2	2	2	1	Защита информационной системы от уроз
3	3	2	1	Схема построения информационной безопасности на уровне государства
4	4	2	1	Анализ способов нарушений
5	5	2	1	Метода криптографии
6	6	1		Основные технологии построения защищенных систем

7	7	4		Концепция информационной безопасности
Итого:		14	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	4	1	Лабораторная работа №2. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей
3	3	4	2	Лабораторная работа №3. Защита программного обеспечения от несанкционированного использования и копирования
4	4	2	2	Лабораторная работа №4. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ
5	5	4	2	Лабораторная работа №5. Разработка и программная реализация криптографических алгоритмов
6	6	2	-	Лабораторная работа №6. Использование функций криптографического интерфейса Windows для защиты информации
7	7	8	2	Лабораторная работа № 7. Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов
Итого:		26	10	

### Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины	Тема			Вид СРС
		ОФО	ЗФО		
1	1	5	7	Информационная безопасность	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
2	2	16	16	Защита информационной системы от уроз	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
3	3	16	16	Схема построения информационной безопасности на уровне государства	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
4	4	14	16	Анализ способов нарушений	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
5	5	5	16	Метода криптографии	Изучение теоретического материала. Выполнение практических заданий с помощью пакетов программ.
6	6	2	9	Основные технологии построения защищенных систем	Изучение теоретического материала.
7	7	5	17	Концепция информационной безопасности	Изучение теоретического материала.
8	К.р.		18		Проведение и подготовка к к.р.
9	Подготовка к экзамену	27	9		Изучение пройденного материала. Подготовка к зачёту.
Итого:		90	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);
- метод проектов (практические занятия).

## **6. Тематика курсовых работ/проектов**

Курсовые работы/проекты учебным планом не предусмотрены.

## **7. Контрольные работы**

7.1. Методические указания для выполнения контрольных работ.

Цель выполнения контрольной работы – закрепление у обучающихся теоретических знаний и приобретение практических навыков применения теории нечётких множеств с помощью пакетов прикладных программ. Контрольная работа состоит из задания и выполненного материала (Графиков, формул и расчётов). Исходными данными для выполнения работы выдаёт преподаватель. По требованию руководителя следует собрать и изучить рекомендуемую литературу, выполнить патентный и тематический поиск информации, в том числе через информационно-телекоммуникационные сети общего доступа. Работа должна включать:

- отчёт с алгоритмами выполненных расчётов. Трудоемкость выполнения контрольной работы – 15 часов.

7.2. Тематика контрольных работ.

- Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними.
- Современные средства защиты информации.
- Современные системы компьютерной безопасности.
- Современные средства противодействия экономическому шпионажу.
- Современные криптографические системы.
- Криптоанализ, современное состояние.
- Правовые основы защиты информации.
- Технические аспекты обеспечения защиты информации. Современное состояние.
- Атаки на систему безопасности и современные методы защиты.
- Современные пути решения проблемы информационной безопасности РФ.

## **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, очно-заочной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
<b>1 текущая аттестация</b>		
	Выполнение лабораторных работ	12
	Защита лабораторных работ	4
	Самостоятельная работа	10
	Практические занятия	5
	<b>ИТОГО за первую текущую аттестацию</b>	<b>31</b>
<b>2 текущая аттестация</b>		
	Выполнение лабораторных работ	12
	Защита лабораторных работ	4
	Самостоятельная работа	10
	Практические занятия	5
	<b>ИТОГО за вторую текущую аттестацию</b>	<b>31</b>
<b>3 текущая аттестация</b>		
	Выполнение лабораторных работ	18
	Защита лабораторных работ	6
	Самостоятельная работа	10
	Практические занятия	4
	<b>ИТОГО за третью текущую аттестацию</b>	<b>38</b>
	<b>ВСЕГО</b>	<b>100</b>

8.3. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся заочной формы обучения представлена в таблице 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
	<b>ИТОГО текущую аттестацию</b>	<b>100</b>

## 9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

№	Профессиональные базы данных и информационные справочные системы	Номер и дата договора	Срок действия договора
1	Научно-техническая библиотека ФГАОУ ВО РГУ Нефти и газа (НИУ) им. И.М. Губкина и ФГБОУ ВО «ТИУ» [электронный ресурс] URL: <a href="http://elib.gubkin.ru/">http://elib.gubkin.ru/</a>	Договор №09-16/19 от 18.10.2019 взаимного оказания услуг двухстороннего доступа к ресурсам	С 18.10.2019 по 17.10.2020
2	Научно-техническая библиотека ФГБОУ ВО РГУ Нефти и газа (НИУ) им. И.М. Губкина [электронный ресурс]. URL: <a href="http://elib.gubkin.ru/">http://elib.gubkin.ru/</a>	Договор № 03-189/2017 от 20.10.2017 об оказании услуг двухстороннего доступа к ресурсам	С 20.10.2017 по 19.10.2019
3	Научно-техническая библиотека ФГБОУ ВПО УГНТУ [электронный ресурс]. URL: <a href="http://bibl.rusoil.net">http://bibl.rusoil.net</a>	Договор № Б173/2017 04-6/2018 от 09.01.2018 на оказание услуг двухстороннего доступа к ресурсам	с 25.12.2017 по 24.12.2019
4	Научно-техническая библиотека ФГБОУ ВПО «Ухтинский государственный технический университет» [электронный ресурс] URL: <a href="http://lib.ugtu.net/books">http://lib.ugtu.net/books</a>	Договор № 04-7/2018 от 15.02.2018 об оказании услуг двухстороннего доступа к ресурсам	С 15.02.2018 по 14.02.2020
5	«Электронная библиотека технического ВУЗа» [электронный ресурс] URL: <a href="http://www.studentlibrary.ru">http://www.studentlibrary.ru</a>	Гражданско-правовой договор № 5064-19 от 31.07.2019 с ООО «Политехресурс» по предоставлению доступа к базе данных Консультант студента	С 01.09.2019 по 31.08.2020
6	Электронно-библиотечная система IPRbooks с ООО Компания «Ай Пи Ар Медиа» [электронный ресурс] URL: <a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>	Договор № 5065-19 от 31.07.2019 на предоставление доступа	С 01.09.2019 по 31.08.2020
7	ЭБС ООО «Издательство ЛАНЬ» [электронный ресурс] URL: <a href="http://e.lanbook.com">http://e.lanbook.com</a>	Гражданско-правовой договор № 5066-19 от 31.07.2019	С 01.09.2019 по 31.08.2020
8	ООО «Электронное издательство ЮРАЙТ» на оказание услуг по предоставлению доступа к ЭБС [электронный ресурс] URL: <a href="http://www.biblio-online.ru">www.biblio-online.ru</a>	Гражданско-правовой договор № 5068-19 от 09.07.2019	С 01.09.2019 по 31.08.2020
9	Электронно-библиотечная система eLibrary с ООО «РУНЭБ» [электронный ресурс] URL: <a href="http://elibrary.ru/">http://elibrary.ru/</a>	Договор №886-18 от 03.12.2018г. на оказание услуг по предоставлению доступа к изданиям Количество пользователей неограниченно, онлайн-доступ с любой точки, где есть Интернет	С 01.01.2019 по 31.12.2019
10	Электронно-библиотечная система BOOK.ru [электронный ресурс] URL: <a href="https://www.book.ru">https://www.book.ru</a>	Гражданско-правовой договор №5931-19 от 29.08.2019 ООО «КноРус медиа» на оказание услуг по предоставлению доступа к электронно-библиотечной системе BOOK.ru	С 01.09.2019 по 31.08.2020
11	Национальная электронная библиотека и	Договор №101НЭБ/6258/09/17/2019 о подключении предоставлении доступа к объектам Национальной электронной библиотеки	С 29.10.2019 по 28.10.2024
12	Полнотекстовая БД ТИУ [электронный ресурс]. URL: <a href="http://elib.tyuiu.ru/">http://elib.tyuiu.ru/</a>		
13	Электронный каталог библиотечно-издательского комплекса ТИУ <a href="http://webirbis.tsogu.ru">http://webirbis.tsogu.ru</a>		
14	Электронный каталог библиотечно-издательского комплекса ТИУ <a href="http://webirbis.tsogu.ru">http://webirbis.tsogu.ru</a>		
15	Единый портал тестирования в сфере образования [электронный ресурс]. URL: <a href="http://www.i-exam.ru">http://www.i-exam.ru</a>		

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

Microsoft Office Professional Plus, договор №5378-19 от 02.09.2019 до 01.09.2020;

2. Microsoft Windows, договор №5378-19 от 02.09.2019 до 01.09.2020.

3. Mathcad 14.0, лицензия PO Number 302/Ni010620, SCN 7A1355535 бессрочно.

## 10. Материально-техническое обеспечение дисциплины

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	Перечень технических средств обучения, необходимых для освоения дисциплины (демонстрационное оборудование)
1		Комплект мультимедийного оборудования: проектор, экран, компьютер, акустическая система. Локальная и корпоративная сеть

## 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. Для эффективной работы обучающиеся должны иметь инженерные калькуляторы и соответствующие канцелярские принадлежности. В процессе подготовки к практическим занятиям 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:

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 нефтегазодобычи» 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). Задания для самостоятельной работы можно найти следующих методических указаниях :

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.

## Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Защита информации в автоматизированных информационных системах

Код, направление подготовки: 09.04.01., Информатика и вычислительная техника

Направленность (профиль): Нейросетевые технологии в автоматизированных системах управления

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
УК-1	Знать: З1 методы анализа своих проблемных ситуаций	Не способен методы анализа своих проблемных ситуаций	Демонстрирует отдельные знания методов анализа своих проблемных ситуаций	Демонстрирует достаточные знания методов анализа своих проблемных ситуаций	Демонстрирует исчерпывающие знания методов анализа своих проблемных ситуаций
	Уметь: У1-принимать решения при проблемных ситуациях	Не способен принимать решения при проблемных ситуаций	Демонстрирует отдельные навыки принимать решения при проблемных ситуаций	Демонстрирует достаточные навыки при принятии решения при проблемных ситуаций	Демонстрирует исчерпывающие навыки при принятии решения при проблемных ситуаций
	Владеть: В1- методами решения при проблемных ситуациях	Не способен владеть методами решения для решения проблемных ситуаций	Демонстрирует владение методами решения для решения проблемных ситуаций	Демонстрирует достаточные владение методами решения для решения проблемных ситуаций	Демонстрирует исчерпывающие владения методами решения для решения проблемных ситуаций
ОПК-1	Знать: З2- методы защиты информации в АИС.	Не способен назвать методы защиты информации в АИС.	Демонстрирует отдельные познания в методах защиты информации в АИС.	Демонстрирует достаточные знания в методах защиты информации в АИС.	Демонстрирует исчерпывающие знания в методах защиты информации в АИС.
	Уметь: У2-применять методы защиты информации в АИС.	Не умеет применять методы защиты информации в АИС.	Частично умеет применять методы защиты информации в АИС.	Умеет применять методы защиты информации в АИС.	В полном объеме умеет может применять методы защиты информации в АИС.
	Владеть:В2-методами защиты информации в АИС.	Не владеет - методами защиты информации в АИС.	Владеет отдельными методами защиты информации в АИС.	В достаточном объеме владеет методами защиты информации в АИС.	В полном объеме владеет методами защиты информации в АИС.

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
ОПК-2	Знать: З3- современные информационные технологии и инструментальные среды защиты информации АИС.	Не знает современные информационные технологии и инструментальные среды защиты информации АИС.	Имеет некоторые познания в информационных технологиях и инструментальных средах защиты информации АИС.	Обладает достаточными познаниями в информационных технологиях и инструментальных средах защиты информации АИС.	Обладает в полном объеме современными в информационных технологиях и инструментальных средах защиты информации АИС.
	Уметь: У3- обосновывать выбор современных информационных технологий защиты информации АИС.	Не умеет обосновывать выбор современных информационных технологий защиты информации АИС.	Частично умеет обосновывать выбор современных информационных технологий защиты информации АИС.	Демонстрирует умение обосновывать выбор современных информационных технологий защиты информации АИС.	Демонстрирует в полном объеме умение обосновывать выбор современных информационных технологий защиты информации АИС.
	Владеть: В3- методами разработки программных средств защиты информации АИС.	Не владеет методами разработки программных средств защиты информации АИС	Частично владеет методами разработки программных средств защиты информации АИС	Владеет практически всеми методами разработки программных средств защиты информации АИС	В полном объеме владеет методами разработки программных средств защиты информации АИС
ОПК-5	Знать: З4- современное аппаратно-программное обеспечение защиты информации в АИС	Не знает современное аппаратно-программное обеспечение защиты информации в АИС	Частично знает современное аппаратно-программное обеспечение защиты информации в АИС	Обладает достаточным объемом знаний современного аппаратно-программного обеспечения защиты информации в АИС	Обладает в полном объеме владеет знаниями современного аппаратно-программного обеспечения защиты информации в АИС
	Уметь: У4 – модернизировать аппаратно-программное обеспечение защиты информации в АИС	Не умеет модернизировать аппаратно-программное обеспечение защиты информации в АИС	Умеет частично модернизировать аппаратно-программное обеспечение защиты информации в АИС	Умеет модернизировать аппаратно-программное обеспечение защиты информации в АИС	В полном объеме умеет может модернизировать аппаратно-программное обеспечение защиты информации в АИС

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: В4-методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.	Не владеет методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.	Владеет некоторыми методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.	Владеет методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.	В полном объеме владеет методами модернизации аппаратно-программного обеспечения АИС на основе защиты информации.

## КАРТА

## обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Защита информации в автоматизированных информационных системахКод, направление подготовки: 09.04.01., Информатика и вычислительная техникаНаправленность (профиль): Нейросетевые технологии в автоматизированных системах 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	<b>Рябко, Б. Я. Криптографические методы защиты информации</b> / Б. Я. Рябко, А. Н. Фионов. - Издание 2-е, стереотипное. - [Б. м.] : Горячая линия-Телеком, 2017. - 230 с. - URL: <a href="https://e.lanbook.com/book/111097">https://e.lanbook.com/book/111097</a> . - Режим доступа: для автор. пользователей. - ЭБС Лань	ЭР	15	100	+
2	Рябко, Борис Яковлевич. Криптографические методы защиты информации: учебное пособие для студентов вузов, обучающимся по специальностям: "Многоканальные телекоммуникационные системы", "Радиосвязь, радиовещание и телевидение", "Защищенные системы связи" / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - Москва : Горячая линия - Телеком, 2013. - 229 с.	15	15	100	-
3	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	15	100	-
4	Кукина, Е. Г. Введение в криптографию : сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 91 с. Режим доступа: <a href="http://www.iprbookshop.ru/24876.html">http://www.iprbookshop.ru/24876.html</a>	ЭР	15	100	+
5	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	15	100	-

ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ <http://webirbis.tsogu.ru/>

Заведующий кафедрой КС \_\_\_\_\_ О.Н. Кузяков

« 1 » 09 \_\_\_\_\_ 2020г.

Директор БИК \_\_\_\_\_ Д.Х. Каюкова

« 1 » 09 \_\_\_\_\_ 2020 г.

М.П.

