МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:

Председатель КСН

_____ О.М. Барбаков

«17» мая 2019г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Информационная безопасность и защита информации
направление подготовки:	02.03.01 Математика и компьютерные науки
направленность:	Математическое и компьютерное моделирование
форма обучения:	очная

Рабочая программа разработана в соответствии с утвержденным учебным планом от 22.04.2019г. и требованиями ОПОП ВО по направлению подготовки 02.03.01 Математика и компьютерные науки, направленность Математическое и компьютерное моделирование к результатам освоения дисциплины «Информационная безопасность и защита информации».

Рабочая программа рассмотрена на заседании кафедры бизнес-информатики и математики

Протокол № 11 от « 27 » 05 2019 г.

Заведующий кафедрой БИМ _____ О.М. Барбаков

СОГЛАСОВАНО:
Заведующий
выпускающей кафедрой БИМ _____ О.М. Барбаков
«27» 05 2019 г.

Рабочую программу разработал:

Шевелев А.В., к.с.н., доцент кафедры БИМ _____

Арясова Д.В., ст. преподаватель кафедры БИМ _____

1. Цели и задачи освоения дисциплины

Цели дисциплины:

– формирование целостной системы знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты;

– формирование практических навыков по использованию компьютерных систем, сетевых технологий и современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.

Задачи дисциплины:

– сформировать представление об основных направлениях государственной политики в области информационной безопасности, обозначить актуальные нормативно-правовые документы, регулирующие деятельность по защите информации;

– показать свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность;

– раскрыть основное содержание, средства и методы используемых на практике или развиваемых направлений информационной безопасности, показать принципы, стратегии и модели защиты информации;

– показать наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий;

– подготовить студентов к дальнейшему изучению, освоению и участию в разработке проектов обеспечения информационной безопасности при использовании локальных и глобальных сетей в деятельности предприятия и личных целях.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам обязательной части учебного плана.

Необходимыми условиями для освоения дисциплины:

знание

- основные понятия информационной безопасности;
- правовые режимы защиты государственной тайны и конфиденциальной информации;

– базовые принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках;

– возможности применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ;

– проблемы и направления развития системных программных средств обеспечения информационной безопасности

умения:

– применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем;

– выполнять основные этапы решения задач информационной безопасности;

– применять на практике основные общеметодологические принципы теории информационной безопасности;

– пользоваться программными средствами, реализующими основные криптографические функции – ключи, цифровую подпись, разделение доступа;

– применять информационные технологии для решения управленческих задач

владение:

– инструментами реализации механизмов информационной безопасности с использованием современных компьютерных технологий;

– основами защиты информации в сети Интернет;

– навыками самостоятельного овладения новыми знаниями в сфере информационной безопасности;

– умением осуществлять выбор средств современных информационных технологий для защиты информации;

– навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации).

Содержание дисциплины является логическим продолжением содержания дисциплины Информатика и служит основой для освоения дисциплин Архитектура вычислительных систем и компьютерных сетей, Администрирование компьютерных сетей.

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-2 Способен проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности	Знать: ОПК-2.З.1 методы научных исследований в конкретной области профессиональной деятельности	Знать: ОПК-2.З.1.1 возможности применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ
	Уметь: ОПК-2.У.1 решать научные задачи в связи с поставленной целью и в соответствии с выбранной методикой	Уметь: ОПК-2.У.1.1 применять на практике основные общеметодологические принципы теории информационной безопасности
	Владеть: ОПК-2.В.1 навыками научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке ОПК-2.В.2 практическим опытом исследований в конкретной области профессиональной деятельности	Владеть: ОПК-2.В.1.1 инструментами реализации механизмов информационной безопасности с использованием современных компьютерных технологий Владеть: ОПК-2.В.2.1 основами защиты информации в сети интернет
ОПК-3 Способен самостоятельно представлять научные результаты, составлять научные документы и отчеты	Знать: ОПК-3.З.1 принципы построения научной работы, современные методы сбора и анализа полученного материала, способы аргументации	Знать: ОПК-3.З.1.1 базовые принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках
	Уметь: ОПК-3.У.1 представлять научные результаты, составлять научные документы и отчеты	Уметь: ОПК-3.У.1.1 применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем
	Владеть: ОПК-3.В.1 практическим опытом выступлений и научной аргументации в профессиональной деятельности	Владеть: ОПК-3.В.1.1 умением осуществлять выбор средств современных информационных технологий для защиты информации
ОПК-5 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности	Знать: ОПК-5.З.1 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: ОПК-5.З.1.1 проблемы и направления развития системных программных средств обеспечения информационной безопасности
	Уметь: ОПК-5.У.1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уметь: ОПК-5.У.1.1 выполнять основные этапы решения задач информационной безопасности
	Владеть: ОПК-5.В.1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной	Владеть: ОПК-5.В.1.1 навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации)

	безопасности	

4. Объем дисциплины

Общий объем дисциплины составляет 5 зачетных единиц, 180 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
Очная	2/3	34	-	34	112	Экзамен

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	Информационная безопасность и уровни ее обеспечения	8		10	21	39	*ОПК-2.З.1 ОПК-2.У.1 ОПК-2.В.1 ОПК-2.В.2 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1 ОПК-5.З.1 ОПК-5.У.1 ОПК-5.В.1*	лабораторная работа
2	2	Компьютерные вирусы и защита от них	8		10	21	39	*ОПК-2.З.1 ОПК-2.У.1 ОПК-2.В.1 ОПК-2.В.2 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1 ОПК-5.З.1 ОПК-5.У.1 ОПК-5.В.1*	лабораторная работа
3	3	Информационная безопасность вычислительных сетей	9		-	21	30	*ОПК-2.З.1 ОПК-2.У.1 ОПК-2.В.1 ОПК-2.В.2 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1 ОПК-5.З.1 ОПК-5.У.1 ОПК-5.В.1*	лабораторная работа
4	4	Механизмы обеспечения «информационной безопасности»	9		14	22	45	*ОПК-2.З.1 ОПК-2.У.1 ОПК-2.В.1 ОПК-2.В.2 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1 ОПК-5.З.1 ОПК-5.У.1 ОПК-5.В.1*	лабораторная работа
5	Экзамен		-	-	-	27	27	*ОПК-2.З.1 ОПК-2.У.1 ОПК-2.В.1 ОПК-2.В.2 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1 ОПК-5.З.1 ОПК-5.У.1 ОПК-5.В.1*	Экзаменационные вопросы и задания
		Итого:	34	-	34	85	27		

заочная форма обучения (ЗФО): не реализуется

очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Информационная безопасность и уровни ее обеспечения».

Понятие «информационная безопасность». Составляющие информационной безопасности. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности».

Раздел 2. «Компьютерные вирусы и защита от них».

Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.

Раздел 3. «Информационная безопасность вычислительных сетей».

Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.

Раздел 4. «Механизмы обеспечения «информационной безопасности»».

Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).

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	4	-	-	Понятие «информационная безопасность». Составляющие информационной безопасности. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.
2	1	4	-	-	Стандарты информационной безопасности: «Общие

					критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности».
3	2	4	-	-	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов.
4	2	4	-	-	Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.
5	3	3	-	-	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO.
6	3	6	-	-	Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.
7	4	3	-	-	Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.
8	4	6	-	-	Регистрация и аудит. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).
Итого:		34	-	-	X

Практические занятия

Практические занятия учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Наименование лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	1	3	-	-	Понятие «информационная безопасность». Составляющие информационной безопасности. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.
2	1	6	-	-	Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности».
3	2	3	-	-	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов.
4	2	6	-	-	Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.
5	3	3	-	-	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO.
6	3	5	-	-	Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины

					успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.
7	4	3	-	-	Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.
8	4	5	-	-	Регистрация и аудит. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).
Итого:		34	-	-	X

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	10	-	-	Понятие «информационная безопасность». Составляющие информационной безопасности. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.	подготовка к лабораторным работам
2	1	11	-	-	Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности».	подготовка к лабораторным работам
3	2	10	-	-	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов.	подготовка к лабораторным работам
4	2	11	-	-	Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.	подготовка к лабораторным работам
5	3	10	-	-	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO.	подготовка к лабораторным работам
6	3	11	-	-	Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.	подготовка к лабораторным работам
7	4	11	-	-	Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.	подготовка к лабораторным работам
8	4	11	-	-	Регистрация и аудит. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).	подготовка к лабораторным работам
9	1-4	27	-	-		подготовка к экзамену
Итого:		112	-	-	X	X

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

- лекция-диалог;
- выполнение лабораторных работ.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены

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	Лабораторная работа №1	0-10
2	Лабораторная работа №2	0-10
3	Лабораторная работа №3	0-10
	ИТОГО за первую текущую аттестацию	**0 – 30**
2 текущая аттестация		
4	Лабораторная работа №4	0-10
5	Лабораторная работа №5	0-10
6	Лабораторная работа №6	0-5
	ИТОГО за вторую текущую аттестацию	**0 – 25**
3 текущая аттестация		
7	Лабораторная работа №7	0-10
8	Лабораторная работа №8	0-15
9	Лабораторная работа №9	0-15
10	Лабораторная работа №10	0-5
	ИТОГО за третью текущую аттестацию	**0 – 45**
	ВСЕГО	**100**

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:

- Собственная полнотекстовая база (ПБД) БИК ТИУ http://elib.tyuiu.ru/
- Научно-техническая библиотеки ФГБОУ ВО РГУ Нефти и газа (НИУ) им. И.М. Губкина http://elib.gubkin.ru/
- Научно-техническая библиотека ФГБОУ ВПО УГНТУ http://bibl.rusoil.net
- Научно-техническая библиотека ФГБОУ ВПО «Ухтинский государственный технический университет» http://lib.ugtu.net/books
- База данных Консультант «Электронная библиотека технического ВУЗа»
- Электронно-библиотечная система IPRbooks http://www.iprbookshop.ru/
- ООО «Издательство ЛАНЬ» http://e.lanbook.com
- ООО «Электронное издательство ЮРАЙТ» www.biblio-online.ru»
- Электронно-библиотечная система elibrary http://elibrary.ru/
- Электронно-библиотечная система BOOK.ru https://www.book.ru

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

- Microsoft Windows;
- Microsoft Office Professional Plus.

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/модуля	Перечень технических средств обучения, необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
1	-	Комплект мультимедийного оборудования: персональный компьютер, проектор, колонки, интерактивная доска, кондиционер, документкамера, экран, телевизор, микрофон

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение

по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников и монографических работ. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на лабораторном занятии.

В начале лабораторного занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

В конце каждой темы подводятся итоги, предлагаются темы докладов, выносятся вопросы для самоподготовки. Как средство контроля и учета знаний студентов в течение семестра проводятся контрольные работы.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания по курсу алгебры и теории чисел, подготовиться к научно-исследовательской деятельности. В процессе работы на оабораторныз занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

Усвоенный материал необходимо научиться применять при выполнении лабораторных работ.

Успешному осуществлению внеаудиторной самостоятельной работы способствуют тестирования. Они обеспечивают непосредственную связь между студентом и преподавателем (по ним преподаватель судит о трудностях, возникающих у студентов в ходе учебного процесса, о степени усвоения предмета, о помощи, какую надо указать, чтобы устранить пробелы в знаниях); они используются для осуществления контрольных функций.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе

самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и, собственно, конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию, поскольку в первые минуты лекции объявляется тема лекции, формулируется ее основная цель. Без этого дальнейшее восприятие лекции становится сложным. Важно научиться слушать преподавателя во время лекции. Здесь не следует путать такие понятия как слышать и слушать. Слушание лекции состоит из нескольких этапов, начиная от слышания (первый шаг в процессе осмысленного слушания) и заканчивая оценкой сказанного.

Чтобы процесс слушания стал более эффективным, нужно разделять качество общения с лектором, научиться поддерживать непрерывное внимание к выступающему. Для оптимизации процесса слушания следует:

1. научиться выделять основные положения. Нельзя понять и запомнить все, что говорит выступающий, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям;

2. во время лекции осуществлять поэтапный анализ и обобщение, услышанного. Необходимо постоянно анализировать и обобщать положения, раскрываемые в речи говорящего. Стараясь представить материал обобщенно, мы готовим надежную базу для экономной, свернутой его записи. Делать это лучше всего по этапам, ориентируясь на момент логического завершения одного вопроса (подвопроса, тезиса и т.д.) и перехода к другому;

3. готовность слушать выступление лектора до конца.

Слушание является лишь одним из элементов хорошего усвоения лекционного материала.

Поток информации, который сообщается во время лекции необходимо фиксировать, записывать – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.

Главным отличием конспекта лекции от текста является свертывание текста. При ведении конспекта удаляются отдельные слова или части текста, которые не выражают

значимую информацию, а развернутые обороты речи заменяют более лаконичными или же синонимичными словосочетаниями. При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры – очень кратко. Особенно важные моменты лекции, на которые следует обратить особое внимание лектор, как правило, читает в замедленном темпе, что позволяет сделать их запись дословной. Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина Информационная безопасность и защита информации
Код, направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Математическое и компьютерное моделирование

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
ОПК-2	Знать: З.1.1 возможности применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ	Не знает возможности применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ	Демонстрирует знание возможностей применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ	Демонстрирует достаточные знания возможностей применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ	Демонстрирует исчерпывающие знания возможностей применения в работе по защите информации современных программных средств: операционных систем, обслуживающих программ
	Уметь: У.1.1 применять на практике основные общеметодологические принципы теории информационной безопасности	Не умеет решать типовые применять на практике основные общеметодологические принципы теории информационной безопасности	Умеет применять на практике основные общеметодологические принципы теории информационной безопасности, допуская значительные неточности и погрешности	Умеет применять на практике основные общеметодологические принципы теории информационной безопасности, допуская незначительные неточности и погрешности	В совершенстве умеет решать применять на практике основные общеметодологические принципы теории информационной безопасности

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: В.1.1 инструментами реализации механизмов информационной безопасности с использованием современных компьютерных технологий В.2.1 основами защиты информации в сети интернет	Не владеет навыками реализации механизмов информационной безопасности с использованием современных компьютерных технологий и основами защиты информации в сети интернет	Владеет навыками реализации механизмов информационной безопасности с использованием современных компьютерных технологий основами защиты информации в сети интернет, допуская значительные ошибки в расчетах	Хорошо владеет навыками реализации механизмов информационной безопасности с использованием современных компьютерных технологий основами защиты информации в сети интернет, допуская незначительные ошибки	В совершенстве владеет навыками реализации механизмов информационной безопасности с использованием современных компьютерных технологий основами защиты информации в сети интернет
ОПК-3	Знать: З.1.1 базовые принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках	Не знает базовые принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках	Демонстрирует знание базовых принципов организации и алгоритмов функционирования систем безопасности в современных операционных системах и оболочках	Демонстрирует достаточные знания базовых принципов организации и алгоритмов функционирования систем безопасности в современных операционных системах и оболочках	Демонстрирует исчерпывающие знания базовых принципов организации и алгоритмов функционирования систем безопасности в современных операционных системах и оболочках
	Уметь: У.1.1 применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем	Не умеет применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем	Умеет применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем, допуская значительные неточности и погрешности	Умеет применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем, допуская незначительные неточности и погрешности	В совершенстве умеет применять знания при анализе состояния информационной безопасности предприятия (организации) и многопользовательских систем

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: В.1.1 умением осуществлять выбор средств современных информационных технологий для защиты информации	Не владеет умением осуществлять выбор средств современных информационных технологий для защиты информации	Владеет умением осуществлять выбор средств современных информационных технологий для защиты информации, допуская значительные ошибки в расчетах	Хорошо владеет умением осуществлять выбор средств современных информационных технологий для защиты информации, допуская незначительные ошибки	В совершенстве владеет умением осуществлять выбор средств современных информационных технологий для защиты информации
ОПК-5	Знать: З.1.1 проблемы и направления развития системных программных средств обеспечения информационной безопасности	Не знает проблемы и направления развития системных программных средств обеспечения информационной безопасности	Демонстрирует знание проблем и направлений развития системных программных средств обеспечения информационной безопасности	Демонстрирует достаточные знания возможностей проблем и направлений развития системных программных средств обеспечения информационной безопасности	Демонстрирует исчерпывающие знания проблем и направлений развития системных программных средств обеспечения информационной безопасности
	Уметь: У.1.1 выполнять основные этапы решения задач информационной безопасности	Не умеет выполнять основные этапы решения задач информационной безопасности	Умеет выполнять основные этапы решения задач информационной безопасности и, допуская значительные неточности и погрешности	Умеет выполнять основные этапы решения задач информационной безопасности, допуская незначительные неточности и погрешности	В совершенстве умеет выполнять основные этапы решения задач информационной безопасности

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: В.1.1 навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации)	Не владеет навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации)	Владеет навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации), допуская значительные ошибки в расчетах	Хорошо владеет навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации), допуская незначительные ошибки	В совершенстве владеет навыком принимать решения по обеспечению необходимого и достаточного уровня информационной безопасности предприятия (организации)

КАРТА

обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина Информационная безопасность и защита информации
Код, направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Математическое и компьютерное моделирование

№ 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	Монаппа, К. А. Анализ вредоносных программ [Электронный ресурс] / К. А. Монаппа. - Москва: ДМК Пресс, 2019. - 452 с. https://e.lanbook.com/	ЭР*	25	100%	+
2	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург: Лань, 2019. - 324 с. https://e.lanbook.com/	ЭР*	25	100%	+
3	Петренко, В. И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс] : учебное пособие / В. И. Петренко, И. В. Мандрица. - 1-е изд. - [Б. м.] : Лань, 2019. - 108 с. https://e.lanbook.com/	ЭР*	25	100%	+
4	Фомичёв, Владимир Михайлович. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата [Текст] : Учебник / В. М. Фомичёв. - Электрон. дан.col. - М : Издательство Юрайт, 2018. - 245 с. http://www.biblio-online.ru/	ЭР*	25	100%	+
5	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров. - 4-е изд., стер. - [Б. м.] : Лань, 2018. - 324 с. https://e.lanbook.com/	ЭР*	25	100%	+

Заведующий кафедрой БИМ _____ О.М. Барбаков
«27» мая 2019 г.

Директор БИК _____ Д.Х. Каюкова
«27» мая 2019 г.
М.П.

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Информационная безопасность и защита информации
Код, направление подготовки: 02.03.01 Математика и компьютерные науки
Направленность: Математика и компьютерное моделирование

№ 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	Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. - 2-е изд., испр. - Санкт-Петербург: Лань, 2020. - 124 с. https://e.lanbook.com	ЭР*	30	100%	+
2	Щеглов, Андрей Юрьевич. Защита информации: основы теории: учебник / Щеглов А. Ю., Щеглов К. А. - Москва: Издательство Юрайт, 2020. - 309 с. https://urait.ru	ЭР*	30	100%	+
3	Запечников, Сергей Владимирович. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва: Юрайт, 2020. - 309 с. https://urait.ru	ЭР*	30	100%	+
4	Бабенко, Людмила Клементьевна. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020. - 220 с. https://urait.ru	ЭР*	30	100%	+
5	Лось, Алексей Борисович. 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, 2020. - 473 с. https://urait.ru	ЭР*	30	100%	+
6	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - Саратов: Профобразование, 2019. - 702 с. http://www.iprbookshop.ru	ЭР*	30	100%	+
7	Лапонина,, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О. Р. Лапонина; под редакцией В. А. Сухомлина. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 605 с. http://www.iprbookshop.ru	ЭР*	30	100%	+

Заведующий кафедрой БИМ _____ О.М. Барбаков
«28» 08 2020 г.

Директор БИК _____ Д.Х. Каюкова
«28» 08 2020 г.
М.П.

Согласовано Вед. [illegible] А. Синицына

Приложение 2

КАРТА

обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Информационная безопасность и защита информации
Код, направление подготовки: 02.03.01 Математика и компьютерные науки
Направленность: Математика и компьютерное моделирование

№ 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	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169817	ЭР*	30	100%	+
2	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469866	ЭР*	30	100%	+
3	Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/468902	ЭР*	30	100%	+
4	Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2020. — 220 с. — (Высшее образование). — ISBN 978-5-9916-9244-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/452871	ЭР*	30	100%	+
5	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., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469133	ЭР*	30	100%	+
6	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html	ЭР*	30	100%	+
7	Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97571.html	ЭР*	30	100%	+

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

Заведующий кафедрой БИМ _____ О.М. Барбаков
«30» августа 2021 г.

Директор БИК _____ Д.Х. Каюкова
«30» августа 2021 г.

Согласовано БИК Директор М.Н. Вайнберг

Дополнения и изменения
к рабочей учебной программе по дисциплине
Информационная безопасность и защита информации
на 2020/2021 учебный год

В рабочую учебную программу вносятся следующие дополнения (изменения):

1. Актуализирована карта методического обеспечения.
2. Внесены изменения в базы данных и информационные справочные системы:
   - Электронно-библиотечная система (обеспечивающая доступ, в том числе к профессиональным базам данных) «Электронного издательства ЮРАЙТ» изменила адрес сайта – www.urait.ru
   - Электронный каталог/Электронная библиотека Тюменского индустриального университета, адрес сайта – www.webirbis.tsogu.ru
   - Электронно – библиотечная система (обеспечивающая доступ, в том числе к профессиональным базам данных) «Консультант студента» добавился адрес сайта – www.studentlibrary.ru
   - Национальная электронная библиотека (НЭБ), адрес сайта – www.rusneb.ru

Дополнения и изменения внес

ст. преподаватель кафедры БИМ _____/ Д.В. Арясова
(подпись)

Дополнения (изменения) в рабочую учебную программу рассмотрены и одобрены на заседании кафедры БИМ. Протокол от «28» ___08___2020г. № 1.

Заведующий кафедрой БИМ _____/ О.М. Барбаков
(подпись)

СОГЛАСОВАНО:

Заведующий
выпускающей кафедрой БИМ _____/ О.М. Барбаков
(подпись)

«28» ___08___2020г.

Дополнения и изменения
к рабочей программе дисциплины
Информационная безопасность и защита информации
на 2021 - 2022 учебный год

В рабочую программу вносятся следующие дополнения (изменения):

1. Актуализирована карта методического обеспечения.
2. Для эффективной организации образовательного процесса при проведении онлайн - занятий в материально – техническое обеспечение дисциплины добавляется бесплатная версия свободно – распространяемого ПО – ZOOM.
3. На основании приказа Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1456 вводится изменение в разделе №3 «Результаты обучения по дисциплине» таблица 3.1:

строку

ОПК-5. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности	Знать: ОПК-5.З.1 Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	Уметь: ОПК-5.У.1 Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	Владеть: ОПК-5.В.1 Иметь навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

заменить на строку

ОПК-5. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-5.З.1Знает принципы работы современных информационных технологий
	ОПК-5.У.1Умеет использовать принципы работы современных информационных технологий для решения практических задач
	ОПК-5.В.1Владеет навыками использованных современных технологий в профессиональной деятельности

Дополнения и изменения внес:
Старший преподаватель кафедры БИМ _____ / А.Н. Величко

Дополнения (изменения) в рабочую учебную программу рассмотрены и одобрены на заседании кафедры БИМ. Протокол от « 30 » августа 2020 г. № 1.

Заведующий кафедрой БИМ _____/ О.М. Барбаков

СОГЛАСОВАНО:

Заведующий
выпускающей кафедрой БИМ _____/О.М. Барбаков
« 30 » августа 2021 г.