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

УТВЕРЖДАЮ

_____

«_____» _____ 20____ г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	«Основы информационной безопасности»
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность:	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена
на заседании кафедры математики м прикладных информационных технологий

Протокол №___от_____2024г.

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины: овладение теоретическими знаниями и умениями, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности в условиях существования угроз безопасности информации.

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ обеспечения информационной безопасности;
- формирование умений выявления и формулирования требований к обеспечению информационной безопасности;
- формирование умений планирования, реализации, и контроля процесса управления информационной безопасностью;
- формирование навыков проведения работ по обеспечению информационной безопасности;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

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 – 2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК – 2.2. Выбирает оптимальный способ решения задач, исходя из имеющихся ресурсов и ограничений	Знать (З1) теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач
		Владеть (В1) практическими навыками оценки рисков безопасности обработки информации
	УК – 2.3. Анализирует действующее законодательство и правовые нормы, регулирующие область профессиональной деятельности	Знать (З2) организационно-правовые основы обеспечения информационной безопасности
		Уметь (У2) планировать и организовывать мероприятия по обеспечению информационной

		безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности
		Владеть (В2) практическими навыками защиты авторских прав и интеллектуальной собственности
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать (З3) теоретические основы управления информационной безопасностью
		Уметь (У3) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения
		Владеть (В3) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единиц, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	2/3	18	-	34	56	-	зачет
заочная	-	-	-	-	-	-	-

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Общие положения информационной безопасности	3	-	5	9	17	УК-2.2 УК-2.3 ПКС-1.1	Задание на лабораторную работу
2	2	Разработка системы управления информационной безопасностью	5	-	7	11	23		Задание на лабораторную работу
3	3	Внедрение и обеспечение функционирования системы управления информационной	3	-	7	11	21		Задание на лабораторную работу

		безопасностью							
4	4	Проведение мониторинга и анализа системы управления информационной безопасностью	2	-	5	8	15		Задание на лабораторную работу
5	5	Поддержка и улучшение системы управления информационной безопасностью	2	-	5	8	15		Задание на лабораторную работу
6	6	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	3	-	5	9	17		Задание на лабораторную работу
7	Зачет		-	-	-	-	-	УК-2.2 УК-2.3 ПКС-1.1	Вопросы к зачету
Итого:			18		34	56	108	-	-

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. «Общие положения информационной безопасности». Основные понятия в области информационной безопасности. Нормативно-правовые акты, специальные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.

Раздел 2. «Разработка системы управления информационной безопасностью». Область и границы действия системы управления информационной безопасностью. Методика оценки угроз безопасности информации. Уязвимости. Оценка и варианты обработки рисков информационной безопасности. Выбор целей и мер управления для обработки рисков информационной безопасности, утверждение остаточных рисков информационной безопасности.

Раздел 3. «Внедрение и обеспечение функционирования системы управления информационной безопасностью». Разработка и реализация плана обработки рисков информационной безопасности. Внедрение мер управления информационной безопасностью. Организационно-технические аспекты обеспечения информационной безопасности. Технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность. Управление работой и ресурсами системы управления информационной безопасностью. Обнаружение событий информационной безопасности и реагирование на инциденты.

Раздел 4. «Проведение мониторинга и анализа системы управления информационной безопасностью». Процедуры мониторинга и анализа результативности системы управления информационной безопасностью. Внутренний аудит системы управления информационной безопасностью. Регистрация действий и событий информационной безопасности.

Раздел 5. «Поддержка и улучшение системы управления информационной безопасностью». Выявление возможности улучшения системы управления информационной безопасностью. Корректирующие и предупреждающие действия. Внедрение улучшений.

Раздел 6. «Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий». Охраняемые результаты интеллектуальной деятельности и средства индивидуализации. Споры, связанные с защитой интеллектуальных прав. Защита интеллектуальных прав. Защита личных неимущественных прав. Защита исключительных прав. Особенности защиты прав лицензиата. Технические средства защиты авторских прав и интеллектуальной собственности.

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	3	-	-	Общие положения информационной безопасности
2	2	5	-	-	Разработка системы управления информационной безопасностью
3	3	3	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	2	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	2	-	-	Поддержка и улучшение системы управления информационной безопасностью
6	6	3	-	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		18	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Общие положения информационной безопасности
2	2	7	-	-	Разработка системы управления информационной безопасностью
3	3	7	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	5	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	5	-	-	Поддержка и улучшение системы управления информационной безопасностью
6	6	5	-	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		34	-	-	-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№	Номер раздела	Объем, час.	Тема	Вид СРС

п/п	дисциплины	ОФО	ЗФО	ОФО		
1	1	9	-	-	Общие положения информационной безопасности	Подготовка к лабораторным работам
2	2	11	-	-	Разработка системы управления информационной безопасностью	Подготовка к лабораторным работам
3	3	11	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью	Подготовка к лабораторным работам
4	4	8	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью	Подготовка к лабораторным работам
5	5	8	-	-	Поддержка и улучшение системы управления информационной безопасностью	Подготовка к лабораторным работам
6	6	9	-	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	Подготовка к лабораторным работам
7	1-6	-	-	-	1-6	Подготовка к зачету
Итого:		56	-	-		

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

- информационно-телекоммуникационная (лекционные занятия, практические занятия)
- групповая (практические занятия)
- индивидуальная (практические занятия)
- рейтинговая (практические занятия)

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	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	**0-30**
2 текущая аттестация		
3	Лабораторная работа № 3	0-15

4	Лабораторная работа № 4	0-15
	ИТОГО за вторую текущую аттестацию	**0-30**
3 текущая аттестация		
5	Лабораторная работа № 5	0-20
6	Лабораторная работа № 6	0-20
	ИТОГО за третью текущую аттестацию	**0-40**
	ВСЕГО	**0-100**

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:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;
- Научно-техническая библиотека РГУ Нефти и газа им. И.М. Губкина http://elib.gubkin.ru/;
- Научно-техническая библиотека УГНТУ http://bibl.rusoil.net;
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books;
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;
- Электронно-библиотечная система «Лань» https://e.lanbook.com;
- Образовательная платформа ЮРАЙТ www.urait.ru;
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;
- Национальная электронная библиотека НЭБ.

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

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- OpenVAS;
- Nmap;
- Wireshark;
- John the Ripper;
- Snort;
- SecretNetStudio;
- VipNet;
- OpenVPN;
- КриптоПро;

10. Материально-техническое обеспечение дисциплины

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

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Основы информационной безопасности	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; 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., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70.
		Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70

11. Методические указания по организации СРС

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

Практические занятия способствуют углублённому изучению дисциплины и служат основной формой подведения итогов самостоятельной работы студентов. Цель практических занятий заключается в углублении и закреплении теоретических знаний, а также в формировании практических компетенций, необходимых будущим специалистам.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику будущих функциональных обязанностей обучающихся, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Студенту рекомендуется следующая схема подготовки к занятию:

- проработать конспект лекций;
- изучить рекомендованную литературу;
- при затруднениях сформулировать вопросы к преподавателю;
- после выполнения практического задания оформить отчет и подготовиться к защите.

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. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с теоретическими источниками. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом 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.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать теоретические знания, подготовиться к научно-исследовательской деятельности. В процессе работы на лабораторных 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 решении проставленных задач.

Успешному осуществлению внеаудиторной самостоятельной работы способствует проведение коллоквиумов. 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 заданий 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: «Основы информационной безопасности»
Код, направление подготовки: 09.03.01 «Информатика и вычислительная техника»
Направленность (профиль): «Информационная безопасность компьютерных систем и сетей»

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК – 2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК – 2.2. Выбирает оптимальный способ решения задач, исходя из имеющихся ресурсов и ограничений	Знать (З1) теоретические основы обеспечения информационной безопасности	Не знает теоретические основы обеспечения информационной безопасности	Знает на низком уровне теоретические основы обеспечения информационной безопасности	Знает на среднем уровне теоретические основы обеспечения информационной безопасности	Знает на высоком уровне теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач	Не умеет планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач	Умеет на низком уровне планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач	Умеет на среднем уровне планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач	Умеет на высоком уровне планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе обработки информации, необходимой для решения поставленных задач
		Владеть (В1) практическими навыками оценки рисков безопасности обработки информации	Не владеет практическими навыками оценки рисков безопасности обработки информации	Владеет на низком уровне практическими навыками оценки рисков безопасности обработки информации	Владеет на среднем уровне практическими навыками оценки рисков безопасности обработки информации	Владеет на высоком уровне практическими навыками оценки рисков безопасности обработки информации
	УК – 2.3. Анализирует действующее законодательство и правовые нормы, регулирующие область профессионал	Знать (З2) организационно-правовые основы обеспечения информационной безопасности	Не знает организационно-правовые основы обеспечения информационной безопасности	Знает на низком уровне организационно-правовые основы обеспечения информационной безопасности	Знает на среднем уровне организационно-правовые основы обеспечения информационной безопасности	Знает на высоком уровне организационно-правовые основы обеспечения информационной безопасности

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
	ьной деятельности	Уметь (У2) планировать и организовывать мероприятия по обеспечению информационной безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности	Не умеет планировать и организовывать мероприятия по обеспечению информационной безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности	Умеет на низком уровне планировать и организовывать мероприятия по обеспечению информационной безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности	Умеет на среднем уровне планировать и организовывать мероприятия по обеспечению информационной безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности	Умеет на высоком уровне планировать и организовывать мероприятия по обеспечению информационной безопасности с учетом действующего законодательства и правовых норм, регулирующих область профессиональной деятельности
		Владеть (В2) практическими навыками защиты авторских прав и интеллектуальной собственности	Не владеет практическими навыками защиты авторских прав и интеллектуальной собственности	Владеет на низком уровне практическими навыками защиты авторских прав и интеллектуальной собственности	Владеет на среднем уровне практическими навыками защиты авторских прав и интеллектуальной собственности	Владеет на высоком уровне практическими навыками защиты авторских прав и интеллектуальной собственности
ПКС-1. Способен обеспечивать информационную безопасность компьютерных	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и	Знать (З3) теоретические основы управления информационной безопасностью	Не знает теоретические основы управления информационной безопасностью	Знает на низком уровне теоретические основы управления информационной безопасностью	Знает на среднем уровне теоретические основы управления информационной безопасностью	Знает на высоком уровне теоретические основы управления информационной безопасностью

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
систем и сетей.	управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Уметь (У3) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Не умеет планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на низком уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на среднем уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на высоком уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения
		Владеть (В3) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Не владеет практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет на низком уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет на среднем уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях	Владеет на высоком уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных; предотвращения потери и повреждения данных при сбоях

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: «Основы информационной безопасности»
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): «Информационная безопасность компьютерных систем и сетей»

№ 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	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557073	ЭР*	30	100	+
2	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268	ЭР*	30	100	+
3	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300	ЭР*	30	100	+
4	Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/15449	ЭР*	30	100	+

5	Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87643.html	ЭР*	30	100	+
6	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095	ЭР*	30	100	+
7	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 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html	ЭР*	30	100	+
8	Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142285.html	ЭР*	30	100	+
9	Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267	ЭР*	30	100	+

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

Лист согласования 00ДО-0000755166

Внутренний документ "ОИБ_2024_09.03.01_ИБКСб"

Ответственный: Кармацкая Елена Александровна

Согласовано

Серийный номер ЭП	Должность	ФИО	ИО	Виза	Комментарий	Дата
	Заведующий кафедрой, имеющий ученую степень доктора наук	Барбаков Олег Михайлович		Согласовано		
	Директор	Каюкова Дарья Хрисановна		Согласовано	Отредактировано	
	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		