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

УТВЕРЖДАЮ

_____

«_____» _____ 20____ г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Информационная безопасность и защита информации
направление подготовки:	38.03.05 Бизнес - информатика
Направленность (профиль):	Информационные системы предприятия
форма обучения:	Очная

Рабочая программа рассмотрена
на заседании кафедры бизнес-информатики и математики

Заведующий кафедрой _____ О.М. Барбаков
(подпись)

Рабочую программу разработал:

А.Н. Величко, старший преподаватель _____
(подпись)

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 обязательной части учебного плана.

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 – 2.1. Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	Знать (З1) теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности
		Владеть (В1) практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности
ОПК – 3. Способен управлять процессами создания и использования продуктов и	ОПК – 3.2 Выбирает оптимальные языки программирования и успешно организует работу с базами данных,	Знать (З2) теоретические основы обеспечения информационной безопасности операционных систем и

услуг в сфере информационно – коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	операционными системами и оболочками, современными программными средами разработки информационных систем и технологий	баз данных
		Уметь (У2) определять угрозы информационной безопасности операционных систем и баз данных
		Владеть (В2) практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности
	ОПК – 3.3 Эффективно использует языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес – процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ	Знать (З3) технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность
		Уметь (У3) определять угрозы надежности и безопасности программного обеспечения
		Владеть (В3) практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования
	ОПК – 3.4 Использует основные методы программирования, отладки и тестирования прототипов программно – технических комплексов задач	Знать (З4) технологии оценки рисков информационной безопасности при разработке ИС
		Уметь (У4) определять требования к ИС с учетом угроз информационной безопасности
		Владеть (В4) практическими навыками восстановления ИС после сбоев

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	3/6	16	-	32	33	27	экзамен

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.	Контроль, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.					
1	1	Общие положения информационной безопасности	3	-	5	5	-	13	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Задание на лабораторную работу, вопросы для защиты
2	2	Разработка системы управления информационной	3	-	7	6	-	16	УК-2.1 ОПК-3.2 ОПК-3.3	Задание на лабораторную работу, вопросы

		безопасностью							ОПК-3.4	для защиты
3	3	Внедрение и обеспечение функционирования системы управления информационной безопасностью	3	-	6	6	-	15	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Задание на лабораторную работу, вопросы для защиты
4	4	Проведение мониторинга и анализа системы управления информационной безопасностью	2	-	5	5	-	12	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Задание на лабораторную работу, вопросы для защиты
5	5	Поддержка и улучшение системы управления информационной безопасностью	2	-	4	5	-	11	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Задание на лабораторную работу, вопросы для защиты
6	6	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	3	-	5	6	-	14	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Задание на лабораторную работу, вопросы для защиты
7	Экзамен						27	27	УК-2.1 ОПК-3.2 ОПК-3.3 ОПК-3.4	Вопросы к экзамену
Итого:			16		32	33	27	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	3	-	-	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:		16	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Общие положения информационной безопасности
2	2	7	-	-	Разработка системы управления информационной безопасностью
3	3	6	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	5	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	4	-	-	Поддержка и улучшение системы управления информационной безопасностью

6	6	5	-	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		32	-	-	-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	5	-	-	Общие положения информационной безопасности	Подготовка к лабораторным работам, оформление отчетов
2	2	6	-	-	Разработка системы управления информационной безопасностью	Подготовка к лабораторным работам, оформление отчетов
3	3	6	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью	Подготовка к лабораторным работам, оформление отчетов
4	4	5	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью	Подготовка к лабораторным работам, оформление отчетов
5	5	5	-	-	Поддержка и улучшение системы управления информационной безопасностью	Подготовка к лабораторным работам, оформление отчетов
6	6	6	-	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	Подготовка к лабораторным работам, оформление отчетов
7	1-6	-	-	-	1-6	Подготовка к экзамену
Итого:		33	-	-		

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

- ИКТ – технологии (визуализация учебного материала в PowerPoint в диалоговом режиме);
- обучение в сотрудничестве (коллективная, групповая работа);
- технология проблемного обучения.

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/;

– Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;

– Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;

– Электронно-библиотечная система «ЛАНЬ» https://e.lanbook.com;

– Образовательная платформа ЮРАЙТ www.urait.ru;

– Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;

– Библиотеки нефтяных вузов России:

- Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/;
- Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/;
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books;

– Электронная справочная система нормативно-технической документации «Технорматив»;

– ЭКБСОН – информационная система доступа к электронным каталогам библиотек сферы образования и науки.

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

- 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)
	2	3	4
1	Информационная безопасность и защита информации	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья.	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:	625039, г. Тюмень, ул. Мельникайте, д. 70

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. 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 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.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать 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.

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, изучение мультимедиалекций, расположенных в свободном доступе, решение ситуационных (профессиональных) задач, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: «Информационная безопасность и защита информации»
Код, направление подготовки: 38.03.05 «Бизнес - информатика»
Направленность (профиль): «Информационные системы предприятия»

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 – 2.1. Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	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 в совершенстве теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности	Не умеет планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности	Умеет на низком уровне планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности	Умеет на среднем уровне планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности	Умеет в совершенстве планировать и организовывать мероприятия по обеспечению информационной безопасности в процессе профессиональной деятельности
		Владеть (В1) практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности	Не владеет практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности	Владеет на низком уровне практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности	Владеет на среднем уровне практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности	Владеет в совершенстве практическими навыками определения требований к информационным системам и оценке рисков их использования с учетом требований информационной безопасности

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ОПК – 3. Способен управлять процессами создания и использования продуктов и услуг в сфере информационно – коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК – 3.2 Выбирает оптимальные языки программирования и успешно организует работу с базами данных, операционными системами и оболочками, современными программными средами разработки информационных систем и технологий	Знать (З2) теоретические основы обеспечения информационной безопасности операционных систем и баз данных	Не знает теоретические основы обеспечения информационной безопасности операционных систем и баз данных	Знает на низком уровне теоретические основы обеспечения информационной безопасности операционных систем и баз данных	Знает на среднем уровне теоретические основы обеспечения информационной безопасности операционных систем и баз данных	Знает в совершенстве теоретические основы обеспечения информационной безопасности операционных систем и баз данных
		Уметь (У2) определять угрозы информационной безопасности операционных систем и баз данных	Не умеет определять угрозы информационной безопасности операционных систем и баз данных	Умеет на низком уровне определять угрозы информационной безопасности операционных систем и баз данных	Умеет на среднем уровне определять угрозы информационной безопасности операционных систем и баз данных	Умеет в совершенстве определять угрозы информационной безопасности операционных систем и баз данных
		Владеть (В2) практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности	Не владеет практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности	Владеет на низком уровне практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности	Владеет на среднем уровне практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности	Владеет в совершенстве практическими навыками защиты операционных систем и баз данных от угроз информационной безопасности
	ОПК – 3.3 Эффективно использует языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес –	Знать (З3) технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность	Не знает технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность	Знает на низком уровне технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность	Знает на среднем уровне технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность	Знает в совершенстве технологии разработки надежного (безопасного) программного обеспечения и методы проверки программного обеспечения на защищенность

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
	процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ	Уметь (У3) определять угрозы надежности и безопасности программного обеспечения	Не умеет определять угрозы надежности и безопасности программного обеспечения	Умеет на низком уровне определять угрозы надежности и безопасности программного обеспечения	Умеет на среднем уровне определять угрозы надежности и безопасности программного обеспечения	Умеет в совершенстве определять угрозы надежности и безопасности программного обеспечения
		Владеть (В3) практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования	Не владеет практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования	Владеет на низком уровне практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования	Владеет на среднем уровне практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования	Владеет в совершенстве практическими навыками защиты программного обеспечения от несанкционированного доступа, исследования и использования
	ОПК – 3.4 Использует основные методы программирования, отладки и тестирования прототипов программно – технических комплексов задач	Знать (З4) технологии оценки рисков информационной безопасности при разработке ИС	Не знает технологии оценки рисков информационной безопасности при разработке ИС	Знает на низком уровне технологии оценки рисков информационной безопасности при разработке ИС	Знает на среднем уровне технологии оценки рисков информационной безопасности при разработке ИС	Знает в совершенстве технологии оценки рисков информационной безопасности при разработке ИС
		Уметь (У4) определять требования к ИС с учетом угроз информационной безопасности	Не умеет определять требования к ИС с учетом угроз информационной безопасности	Умеет на низком уровне определять требования к ИС с учетом угроз информационной безопасности	Умеет на среднем уровне определять требования к ИС с учетом угроз информационной безопасности	Умеет в совершенстве определять требования к ИС с учетом угроз информационной безопасности
		Владеть (В4) практическими навыками восстановления ИС после сбоев	Не владеет практическими навыками восстановления ИС после сбоев	Владеет на низком уровне практическими навыками восстановления ИС после сбоев	Владеет на среднем уровне практическими навыками восстановления ИС после сбоев	Владеет в совершенстве практическими навыками восстановления ИС после сбоев

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: «Информационная безопасность и защита информации»
Код, направление подготовки: 38.03.05 «Бизнес - информатика»
Направленность (профиль): «Информационные системы предприятия»

№ 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	Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. - Москва: Издательство Юрайт, 2020. - 309 с. - (Бакалавр и магистр. Академический курс). - ЭБС "Юрайт". - ISBN 978-5-534-04732-5 https://urait.ru/bcode/449285	ЭР*	30	100	+
2	Защита информации: учебное пособие для вузов / А. А. Внуков. - 3-е изд., пер. и доп. - Москва: Издательство Юрайт, 2021. - 161 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-534-07248-8 https://urait.ru/bcode/470131	ЭР*	30	100	+
3	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020. - 312 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-9916-9043-0 https://urait.ru/bcode/452368	ЭР*	30	100	+
4	**Нестеров, С. А.** Основы информационной безопасности : учебное пособие для вузов / С. А. Нестеров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2023. - 324 с. - URL: https://e.lanbook.com/book/341267 .	ЭР*	30	100	+
5	Информационная безопасность и защита информации: практикум / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. - Дубна: Государственный университет «Дубна», 2020. - 85 с. - ЭБС "Лань". - ISBN 978-5-89847-608-3 https://e.lanbook.com/book/154490	ЭР*	30	100	+

6	Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020. - 220 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-9916-9244-1 https://urait.ru/bcode/452871	ЭР*	30	100	+
7	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 http://www.iprbookshop.ru/87643.html	ЭР*	30	100	+
8	Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2019. - 344 с. - ЭБС Лань. - ISBN 978-5-8114-3940-9 https://e.lanbook.com/book/125739	ЭР*	30	100	+
9	Информационная безопасность и защита информации / В. Ф. Шаньгин. - Саратов: Профобразование, 2019. - 702 с. - ЭБС "IPR BOOKS". - ISBN 978-5-4488-0070-2 http://www.iprbookshop.ru/87995.html	ЭР*	30	100	+
10	Основы информационной безопасности: учебное пособие / В. А. Галатенко. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Эр Медиа, 2020. - 266 с. - URL: http://www.iprbookshop.ru/97562.html	ЭР*	30	100	+

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