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

УТВЕРЖДАЮ

_____

«_____» _____ 20____ г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Обеспечение безопасности персональных данных
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

Рабочую программу разработал:

А.Н. Величко, старший преподаватель

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 безопасности персональных данных в условиях существования угроз безопасности информации.

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ обеспечения безопасности персональных данных;
- изучение методов и процедур выявления угроз безопасности персональных данных и оценки степени их опасности;
- практическая отработка способов и порядка проведения работ по обеспечению безопасности персональных данных;
- 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 и информационной безопасности;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины является логическим продолжением содержания дисциплины «Информационная безопасность и защита информации» и 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

1. Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
УК – 1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК – 1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в соответствии с требованиями и условиями задачи	Знать (З1) теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации
		Уметь (У1) планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных
		Владеть (В1) практическими навыками определения уровня защиты

		персональных данных; выявления угроз безопасности персональных данных
ПКС – 3. Способен выявлять и анализировать требования к ИС, разрабатывать архитектуру, осуществлять прототипирование, проектирование и дизайн ИС, писать технические задания на разработку ИС, создавать пользовательскую документацию к ИС	ПКС – 3.1 Грамотно оформляет техническую и пользовательскую документацию на различных стадиях жизненного цикла информационных систем	Знать (З2) организационно-правовые основы обеспечения безопасности персональных данных
		Уметь (У2) определять требования к проекту разработки системы обеспечения безопасности персональных данных
		Владеть (В2) практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных

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	4/7	14	-	28	66	-	Зачет

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	Правовые и организационные основы технической защиты информации ограниченного доступа	3	-	5	13	21	УК-1.2 ПКС-3.1	Задание на лабораторную работу
2	2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	3	-	5	14	22	УК-1.2 ПКС-3.1	Задание на лабораторную работу
3	3	Угрозы безопасности	3	-	6	13	22	УК-1.2	Задание на

		персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных						ПКС-3.1	лабораторную работу
4	4	Основы организации и ведения работ по обеспечению безопасности персональных данных	3	-	5	13	21	УК-1.2 ПКС-3.1	Задание на лабораторную работу
5	5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	2	-	7	13	22	УК-1.2 ПКС-3.1	Задание на лабораторную работу
6	Зачет		-	-	-	-	-	УК-1.2 ПКС-3.1	Вопросы к зачету
Итого:			14		28	66	108	X	X

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. Правовые и организационные основы технической защиты информации ограниченного доступа. 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. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Раздел 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа. Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз. Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз.

Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Раздел 3. Угрозы безопасности персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных. Особенности информационного элемента информационной системы персональных данных. Раскрытие понятия актуальных угроз безопасности персональных данных. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Методы и процедуры выявления угроз безопасности персональных данных в информационных системах персональных данных. Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Классификация угроз безопасности и уязвимостей информационной системы персональных данных, а также их характеристики. Описание типовых моделей угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, в зависимости от целей и содержания персональных данных. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам. Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий. Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии. Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Оценка защищенности информации, обрабатываемой основными техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок на вспомогательные технические средства и системы и их коммуникации.

Раздел 4. Основы организации и ведения работ по обеспечению безопасности персональных данных. Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных. Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты пер-

сональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных. Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации. Понятие государственной информационной системы, обрабатывающей персональные данные. Особенности защиты информации, содержащейся в государственной информационной системе персональных данных. Определение класса защищенности государственной информационной системы и необходимых мер по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление. Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Раздел 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных. Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных. Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации. Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

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	-	-	Правовые и организационные основы технической защиты информации ограниченного доступа
2	2	3	-	-	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

3	3	3	-	-	Угрозы безопасности персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных
4	4	3	-	-	Основы организации и ведения работ по обеспечению безопасности персональных данных
5	5	2	-	-	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных
Итого:		14	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Правовые и организационные основы технической защиты информации ограниченного доступа
2	2	5	-	-	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа
3	3	6	-	-	Угрозы безопасности персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных
4	4	5	-	-	Основы организации и ведения работ по обеспечению безопасности персональных данных
5	5	7	-	-	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных
Итого:		28	-	-	-

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	13	-	-	Правовые и организационные основы технической защиты информации ограниченного доступа	Подготовка к лабораторным работам, оформление отчетов
2	2	14	-	-	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Подготовка к лабораторным работам, оформление отчетов
3	3	13	-	-	Угрозы безопасности персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	Подготовка к лабораторным работам, оформление отчетов
4	4	13	-	-	Основы организации и ведения работ по обеспечению безопасности персональных	Подготовка к лабораторным работам, оформление отчетов

					данных	
5	5	13	-	-	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Подготовка к лабораторным работам, оформление отчетов
6	1-5	-	-	-	Зачет	Подготовка к зачету
Итого:		66	-	-		

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	0-40
	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;
- Nmap;
- Snort;
- SecretNetStudio;

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
.	Обеспечение безопасности персональных данных	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:	625039, г. Тюмень, ул.

		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.	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: Обеспечение безопасности персональных данных
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 – 1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК – 1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в соответствии с требованиями и условиями задачи	Знать (З1) теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации	Не знает теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации	Знает на низком уровне теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации	Знает на среднем уровне теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации	Знает в совершенстве теоретические основы планирования, организации и проведения работ по обеспечению безопасности персональных данных в условиях существования угроз безопасности информации
		Уметь (У1) планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных	Не умеет планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных	Умеет на низком уровне планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных	Умеет на среднем уровне планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных	Умеет в совершенстве планировать и организовывать мероприятия по обеспечению безопасности персональных данных, определять состав и содержание мер по обеспечению безопасности персональных данных, необходимых для блокирования угроз безопасности персональных данных

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть (В1) практическими навыками определения уровня защиты персональных данных; выявления угроз безопасности персональных данных	Не владеет практическими навыками определения уровня защиты персональных данных; выявления угроз безопасности персональных данных	Владеет на низком уровне практическими навыками определения уровня защиты персональных данных; выявления угроз безопасности персональных данных	Владеет на среднем уровне практическими навыками определения уровня защиты персональных данных; выявления угроз безопасности персональных данных	Владеет в совершенстве практическими навыками определения уровня защиты персональных данных; выявления угроз безопасности персональных данных
ПКС – 3. Способен выявлять и анализировать требования к ИС, разрабатывать архитектуру, осуществлять прототипирование, проектирование и дизайн ИС, писать технические задания на разработку ИС, создавать пользовательскую документацию к ИС	ПКС – 3.1 Грамотно оформляет техническую и пользовательскую документацию на различных стадиях жизненного цикла информационных систем	Знать (З2) организационно-правовые основы обеспечения безопасности персональных данных	Не знает организационно-правовые основы обеспечения безопасности персональных данных	Знает на низком уровне организационно-правовые основы обеспечения безопасности персональных данных	Знает на среднем уровне организационно-правовые основы обеспечения безопасности персональных данных	Знает в совершенстве организационно-правовые основы обеспечения безопасности персональных данных
		Уметь (У2) определять требования к проекту разработки системы обеспечения безопасности персональных данных	Не умеет определять требования к проекту разработки системы обеспечения безопасности персональных данных	Умеет на низком уровне определять требования к проекту разработки системы обеспечения безопасности персональных данных	Умеет на среднем уровне определять требования к проекту разработки системы обеспечения безопасности персональных данных	Умеет в совершенстве определять требования к проекту разработки системы обеспечения безопасности персональных данных
		Владеть (В2) практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных	Не владеет практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных	Владеет на низком уровне практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных	Владеет на среднем уровне практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных	Владеет в совершенстве практическими навыками оформления технической и пользовательской документации системы обеспечения безопасности персональных данных

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Обеспечение безопасности персональных данных
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	**Скрипник, Д. А.** **Обеспечение безопасности персональных данных** : учебное пособие / Д. А. Скрипник. - 4-е изд. - Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 121 с. - **URL:** https://www.iprbookshop.ru/89449.html. - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	ЭР*	30	100	+
3	**Петренко, В. И.** **Защита персональных данных в информационных системах** : [Электронный ресурс] : учебное пособие / В. И. Петренко. - Ставрополь : Северо-Кавказский федеральный университет, 2016. - 201 с. - **URL:** http://www.iprbookshop.ru/66023.html. - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	ЭР*	30	100	+
4	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	+

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