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

УТВЕРЖДАЮ
Заместитель директора по УМР

_____ Н.В. Зонова
«_____» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Анализ защищенности информационных систем от внешних воздействий**

направление подготовки: **09.03.02 Информационные системы и технологии**

направленность (профиль): **Искусственный интеллект и программирование**

форма обучения: **очная**

Рабочая программа разработана для обучающихся по направлению подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) «Искусственный интеллект и программирование»

Рабочая программа рассмотрена
на заседании кафедры кибернетических систем

Руководитель образовательной программы _____ У. В. Лаптева

Рабочую программу разработали:

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

1. Цели и задачи освоения дисциплины

Целью дисциплины является изучение существующих теоретических и нормативно-правовых аспектов защиты информации, освоение обучающимися методики проведения анализа состояния защиты данных на предприятии или в подразделении.

Задачи дисциплины

– изучение существующих теоретических и нормативно-правовых аспектов защиты информации;

– приобретений практических навыков по применению методики проведения анализа состояния защиты данных (анализ носителей данных, инвентаризация технических средств).

Особенностью дисциплины является то, что после изучения курса обучающиеся будут:

- знать информационные элементы (данные всех видов и на любых носителях, используемые при решении задач в ИС), технические средства (средства ввода, обработки, хранения и вывода данных), которые могут подвергнуться случайному и/или преднамеренному воздействию.

- уметь выявлять реально существующие и потенциально возможные «каналы утечки информации» (направления несанкционированного воздействия на защищаемые элементы).

- владеть навыком анализа степени защищенности ИС, обучающийся сможет оценить эффективность работы существующих средств защиты по перекрытию «каналов утечки информации», выработать рекомендации по дополнительным методам и средствам защиты для устранения обнаруженных дефектов в информационной безопасности и надежного перекрытия каналов утечки.

2. Место дисциплины в структуре ОПОП ВО

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

Необходимыми условиями для освоения дисциплины являются:

- базовыми основами информационного, технического и правового обеспечения информационныzх систем;

- умение осуществлять поиск и анализировать всесторонних системных факторов;

- навык постановки и выполнения методических действий.

Содержание дисциплины является логическим продолжением содержания дисциплин математической, компьютерно – информационной и проектной направленности, может быть использовано для подготовки и написания ВКР.

.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
ПКС-3 Способен подготавливать тестовые данные, выполнять тестовые процедуры, разрабатывать тестовые случаи, проводить тестирования и оценивание результатов, оформлять документацию для тестирования и анализа тестового покрытия	ПКС-3.1 Описывает тестовые случаи в работе информационной системы, подготавливает тесты и проводит тестирование системы, анализирует полученные результаты и составляет отчета о тестировании системы.	Знать: З1 - основные понятия теории информационной безопасности З2 - основные свойства защищаемой информации, виды и формы представления информации
		Уметь: У1 - описывать структура и представляет шкалу ценности информации У2 – проводить инвентаризацию информационных систем
		Владеть: В1 – знаниями государственной политики информационной безопасности

		В2 – навыком классификации угроз информационной безопасности
	ПКС-3.2 Организует определение требований к тестам и выявляет тестовое покрытие, разрабатывает стратегии тестирования и анализа защищенности, контролирует проведения работ по тестированию систем	Знать: З3 - основные принципы построения систем защиты З4 - средства реализации комплексной защиты информации
		Уметь: У3 – выявлять каналы утечки информации
		Владеть: В3 – навыком инвентаризации методов и средств защиты информации В4 – методом оценки уязвимости системы
ПКС-8 Способен собирать, подготавливать, визуализировать данные цифрового следа в соответствии с моделью деятельности человека и информационных систем; осуществлять проверку гипотез на модели, поиск закономерностей, обрабатывать и анализировать данные	ПКС-8.1 Проводит разметку данных и выполняет их поверку на достоверность; разрабатывает метрик и оценивает на основе метрик качество представленного цифрового следа	Знать: З5 - задачи защиты информации З6 – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа
		Уметь: У4 – классифицировать информационные ресурсы У5 – реализовывать политику и модели безопасности
		Владеть: В5 - систематизацией понятий в области защиты информации
	ПКС-8.2 Анализирует данные цифрового следа и визуализирует результаты анализа цифрового следа, осуществляет поиск контекстов и событий в потоке данных цифрового следа	Знать: З7 - предметную область теории информационной безопасности З8 - требования ISO 17799, 270000 и других международных стандартов
		Уметь: У6 – проводить анализ уязвимостей системы У7 – проводить анализ защищенности данных в информационной системе
		Владеть: В6 – навыком реализации ролевой модели безопасности

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	30	–	16	62	–	зачет

5. Структура и содержание дисциплины

5.1. Структура дисциплины

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				

1	1	Основные понятия теории информационной безопасности	4	–	–	8	12	ПКС 3.1 ПКС 3.2 ПКС 8.2	Вопросы к опросу
2	2	Информация как объект защиты	4	–	2	8	14	ПКС 3.1	Вопросы к опросу, отчет по лабораторной работе
3	3	Угрозы информационной безопасности	4	–	4	8	16	ПКС 3.1 ПКС 3.2 ПКС 8.2	Вопросы к опросу, отчет по лабораторной работе
4	4	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	6	–	6	10	22	ПКС 3.2 ПКС 8.1	Вопросы к опросу, отчет по лабораторной работе
5	5	Политика и модели безопасности	6	–	4	10	20	ПКС 8.1 ПКС 8.2	Вопросы к опросу, отчет по лабораторной работе
6	6	Обзор международных стандартов информационной безопасности	6	–	–	8	14	ПКС 8.2	Вопросы к опросу
7	Зачет		–	–	–	10	10	ПКС 3.1 ПКС 3.2 ПКС 8.1 ПКС 8.2	Вопросы к зачету
Итого:			30	–	16	62	108		

заочная форма обучения (ЗФО): не реализуется

очно–заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины

5.2.1. Содержание разделов дисциплины

Раздел 1. «*Основные понятия теории информационной безопасности*». История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.

Раздел 2. «*Информация как объект защиты*». Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной Безопасности: информационная безопасность и ее место в системе

национальной безопасности Российской Федерации; органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

Раздел 3. «*Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности*». Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы. Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

Раздел 4. «*Построение систем защиты от угрозы нарушения целостности информации и отказа доступа*». Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.

Раздел 5. «*Политика и модели безопасности*». Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.

Раздел 6. «*Обзор международных стандартов информационной безопасности*». Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000. Требованиям ISO 17799.

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	Основные понятия теории информационной безопасности	4	–	–	История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации
2	Информация как объект защиты	4	–	–	Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов. Государственная политика

					информационной безопасности. Концепция комплексного обеспечения информационной Безопасности: информационная безопасность и ее место в системе национальной безопасности Российской Федерации; органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность
3	Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности	4	–	–	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы. Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения 6конфиденциальности на уровне содержания информации
4	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	6	–	–	Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации
5	Политика и модели безопасности	6	–	–	Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности
6	Обзор международных стандартов информационной безопасности	6	–	–	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000. Требованиям ISO 17799
Итого:		30	–	–	

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Наименование лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	2	2	–	–	Инвентаризация информационной системы
2	3	4	–	–	Классификация элементов информационной системы
3	4	4	–	–	Выявление каналов утечки информации
4	4	2	–	–	Инвентаризация методов и средств защиты информации
5	5	4	–	–	Анализ защищенности данных в информационной системе
Итого:		16	–	–	

Практические занятия

Практические работы учебным планом не предусмотрены

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	8	–	–	Основные понятия теории информационной безопасности	Проработка литературы и теоретического материала
2	2	8	–	–	Информация как объект защиты	Проработка литературы и теоретического материала. Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
3	3	8	–	–	Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности	Проработка литературы и теоретического материала. Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
4	4	10	–	–	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Проработка литературы и теоретического материала. Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
5	5	10	–	–	Политика и модели безопасности	Проработка литературы и теоретического материала. Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
6	6	8	–	–	Обзор международных стандартов информационной безопасности	Проработка литературы и теоретического материала
7	зачёт	10	–	–		Подготовка к зачёту, проработка материалов
Итого:		62	–	–		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий: практико–модульное, проектно–ориентированное обучение и смешанных (обучение с использованием системы blendedlearning – используются специальные информационные технологии, такие как компьютерная графика, аудио и видео, интерактивные элементы и т.п), обучение в дистанционном формате.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены

7. Контрольные работы для заочной формы обучения

Заочная форма не реализуется

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	Выполнение и защита лабораторных работ №1–2	0–25
2	Опрос по разделам 1-3	0–25
	ИТОГО за первую текущую аттестацию	50
2 текущая аттестация		
3	Выполнение и защита лабораторных работ №3–5	0–25
4	Опрос по разделам 4-6	0–25
	ИТОГО за вторую текущую аттестацию	50
	ВСЕГО	100

9. Учебно–методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы

1 Сайт ФГБОУВО ТИУ – http://www.tyuiu.ru/
2 Система поддержки дистанционного обучения Educon – http://educon2.tyuiu.ru/
3 Электронный каталог Библиотечно–издательского комплекса –http://webirbis.tsogu.ru/
4 Электронная библиотечная система eLib –http://elib.tsogu.ru/
5 Научная электронная библиотека eLibrary.ru –http://elibrary.ru/defaultx.asp
6 ЭБС издательства «Лань» – http://e.lanbook.com
7 Официальный сайт компании «Консультант Плюс» – http://www.consultant.ru
8 Международная Электротехническая Комиссия МЭК – http://www.iec.ch
9 Международная Организация по Стандартизации ISO – http://www.iso.org/iso.ru
10 Единый портал тестирования в сфере образования – http://www.i–exam.ru

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

1 Программный продукт КОНДОР+, разработанный российской компанией Digital Security, предназначен для проверки соответствия политики информационной безопасности компании требованиям ISO 17799.
2 Microsoft Windows;
3 Microsoft Office Professional Plus;

10. Материально–техническое обеспечение дисциплины

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

Таблица 10.1

Обеспеченность материально–технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов,	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной	Адрес (местоположение) помещений для проведения всех

	дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно– наглядных пособий	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	Анализ защищенности информационных систем от внешних воздействий	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Учебная мебель: столы, стулья, доска аудиторная. Моноблок – 1 шт., проектор – 1 шт., акустическая система (колонки) – 4 шт., проекционный экран – 1 шт., документ–камера – 1 шт., телевизор – 2 шт.	625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70
		Лабораторные занятия: Учебная аудитория для проведения занятий семинарского типа (практические и лабораторные занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, Учебная мебель: столы, стулья, доска аудиторная. Моноблок – 16 шт., проектор – 1 шт., акустическая система (колонки) – 4 шт., проекционный экран – 1 шт., документ–камера – 1 шт., телевизор – 2 шт.	625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям. Лабораторные работы по данной дисциплине не предусмотрены учебным планом.

При подготовке к практическим занятиям обучающемуся рекомендуется повторить теоретический лекционный материал, а также прочитать соответствующие темы в основной и дополнительной рекомендуемой литературе. Составить перечень возникших в ходе изучения материала вопросов и обсудить возникшие вопросы с преподавателем до начала выполнения лабораторной работы.

11.2 Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения. Преподаватель на занятии дает рекомендации, необходимые для освоения материала. В ходе самостоятельной работы обучающиеся должны выполнить задания на компьютере с помощью пакетов прикладных программ, изучить теоретический материал по разделам. Обучающиеся должны понимать содержание выполненной работы (знать определения понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п). Более подробно порядок выполнения заданий изложен в следующих методических указаниях:

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Анализ защищенности информационных систем от внешних воздействий
Код, направление подготовки: 09.03.02 Информационные системы и технологии
Направленность (профиль): Искусственный интеллект и программирование

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-3 Способен подготавливать тестовые данные, выполнять тестовые процедуры, разрабатывать тестовые случаи, проводить тестирования и оценивание результатов, оформлять документацию для тестирования и анализа тестового покрытия	ПКС-3.1 Описывает тестовые случаи в работе информационной системы, подготавливает тесты и проводит тестирование системы, анализирует полученные результаты и составляет отчета о тестировании системы.	Знать: З1 - основные понятия теории информационной безопасности З2 - основные свойства защищаемой информации, виды и формы представления информации	Не знает: - основные понятия теории информационной безопасности - основные свойства защищаемой информации, виды и формы представления информации	Знает частично: - основные понятия теории информационной безопасности - основные свойства защищаемой информации, виды и формы представления информации	Знает: - основные понятия теории информационной безопасности - основные свойства защищаемой информации, виды и формы представления информации	Отлично знает: - основные понятия теории информационной безопасности - основные свойства защищаемой информации, виды и формы представления информации
		Уметь: У1 - описывать структура и представляет шкалу ценности информации У2 – проводить инвентаризацию информационных систем	Не умеет: – описывать структура и представляет шкалу ценности информации – проводить инвентаризацию информационных систем	Умеет частично: – описывать структура и представляет шкалу ценности информации – проводить инвентаризацию информационных систем	Умеет: – описывать структура и представляет шкалу ценности информации – проводить инвентаризацию информационных систем	Уверенно умеет: – описывать структура и представляет шкалу ценности информации – проводить инвентаризацию информационных систем
		Владеть: В1 – знаниями государственной политики информационной безопасности В2 – навыком классификации угроз информационной	Не владеет: – знаниями государственной политики информационной безопасности – навыком	Плохо владеет: – знаниями государственной политики информационной безопасности – навыком	Владеет: – знаниями государственной политики информационной безопасности – навыком	Прекрасно владеет: – знаниями государственной политики информационной безопасности

		безопасности	классификации угроз информационной безопасности	классификации угроз информационной безопасности	классификации угроз информационной безопасности	– навыком классификации угроз информационной безопасности
	ПКС-3.2 Организует определение требований к тестам и выявляет тестовое покрытие, разрабатывает стратегии тестирования и анализа защищенности, контролирует проведения работ по тестированию систем	Знать: З3 - основные принципы построения систем защиты З4 - средства реализации комплексной защиты информации	Не знает: - основные принципы построения систем защиты - средства реализации комплексной защиты информации	Знает частично: - основные принципы построения систем защиты - средства реализации комплексной защиты информации	Знает: - основные принципы построения систем защиты - средства реализации комплексной защиты информации	Отлично знает: - основные принципы построения систем защиты - средства реализации комплексной защиты информации
		Уметь: У3 – выявлять каналы утечки информации	Не умеет выявлять каналы утечки информации	Умеет частично выявлять каналы утечки информации	Умеет выявлять каналы утечки информации	Уверенно умеет выявлять каналы утечки информации
		Владеть: В3 – навыком инвентаризации методов и средств защиты информации В4 – методом оценки уязвимости системы	Не владеет: – навыком инвентаризации методов и средств защиты информации – методом оценки уязвимости системы	Плохо владеет: – навыком инвентаризации методов и средств защиты информации – методом оценки уязвимости системы	Владеет: – навыком инвентаризации методов и средств защиты информации – методом оценки уязвимости системы	Прекрасно владеет: – навыком инвентаризации методов и средств защиты информации – методом оценки уязвимости системы
ПКС-8 Способен собирать, подготавливать, визуализировать данные цифрового следа в соответствии с моделью деятельности человека и информационных систем; осуществлять проверку гипотез на	ПКС-8.1 Проводит разметку данных и выполняет их поверку на достоверность; разрабатывает метрик и оценивает на основе метрик качество представленного цифрового следа	Знать: З5 - задачи защиты информации З6 – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа	Не знает: - задачи защиты информации – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа	Знает частично: - задачи защиты информации – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа	Знает: - задачи защиты информации – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа	Отлично знает: - задачи защиты информации – подходы к построению систем защиты от угрозы нарушения целостности информации и отказа доступа
		Уметь: У4 – классифицировать информационные ресурсы	Не умеет: – классифицировать	Умеет частично: – классифицировать	Умеет: – классифицировать	Уверенно умеет: – классифицировать

модели, поиск закономерностей, обрабатывать и анализировать данные		У5 – реализовывать политику и модели безопасности	информационные ресурсы – реализовывать политику и модели безопасности	информационные ресурсы – реализовывать политику и модели безопасности	информационные ресурсы – реализовывать политику и модели безопасности	информационные ресурсы – реализовывать политику и модели безопасности
		Владеть: В5 - систематизацией понятий в области защиты информации	Не владеет систематизацией понятий в области защиты информации	Плохо владеет систематизацией понятий в области защиты информации	Владеет систематизацией понятий в области защиты информации	Прекрасно владеет систематизацией понятий в области защиты информации
	ПКС-8.2 Анализирует данные цифрового следа и визуализирует результаты анализа цифрового следа, осуществляет поиск контекстов и событий в потоке данных цифрового следа	Знать: З7 - предметную область теории информационной безопасности З8 - требования ISO 17799, 270000 и других международных стандартов	Не знает: - предметную область теории информационной безопасности - требования ISO 17799, 270000 и других международных стандартов	Знает частично: - предметную область теории информационной безопасности - требования ISO 17799, 270000 и других международных стандартов	Знает: - предметную область теории информационной безопасности - требования ISO 17799, 270000 и других международных стандартов	Отлично знает: - предметную область теории информационной безопасности - требования ISO 17799, 270000 и других международных стандартов
		Уметь: У6 – проводить анализ уязвимостей системы У7 – проводить анализ защищенности данных в информационной системе	Не умеет: – проводить анализ уязвимостей системы – проводить анализ защищенности данных в информационной системе	Умеет частично: – проводить анализ уязвимостей системы – проводить анализ защищенности данных в информационной системе	Умеет: – проводить анализ уязвимостей системы – проводить анализ защищенности данных в информационной системе	Уверенно умеет: – проводить анализ уязвимостей системы – проводить анализ защищенности данных в информационной системе
		Владеть: В6 – навыком реализации ролевой модели безопасности	Не владеет навыком реализации ролевой модели безопасности	Плохо владеет навыком реализации ролевой модели безопасности	Владеет навыком реализации ролевой модели безопасности	Прекрасно владеет навыком реализации ролевой модели безопасности

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно–методической литературой

Дисциплина: **Анализ защищенности информационных систем от внешних воздействий**
Код, направление подготовки: **09.03.02 Информационные системы и технологии**
Направленность (профиль): **Искусственный интеллект и программирование**

№ 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	Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / составители В. В. Денисов. — Новосибирск : Новосибирский государственный технический университет, 2012. — 52 с. — ISBN 978-5-7782-1969-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/44897.html. — Режим доступа: для авторизир. пользователей	ЭР	25	100	+
2	Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 201 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66023.html. — Режим доступа: для авторизир. пользователей	ЭР	25	100	+
3	Петренко, В. И. Защита персональных данных в информационных системах : лабораторный практикум / В. И. Петренко, И. В. Мандрица. — Ставрополь : Северо-Кавказский федеральный университет, 2018. — 118 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/83198.html. — Режим доступа: для авторизир. пользователей	ЭР	25	100	+
4	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	25	100	+

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