Бюджетное учреждение высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

13 июня 2024г., протокол УМС №5

МОДУЛЬ ДИСЦИПЛИН ПРОФИЛЬНОЙ НАПРАВЛЕННОСТИ
Управление корпоративной информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план g090402-УпрДан-24-2.plx
09.04.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Управление данными

Квалификация **Магистр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану	180	Виды контроля	в семестрах:
в том числе:		экзамены	3
аудиторные занятия	32		
самостоятельная работа	103		
часов на контроль	45		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	17 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	103	103	103	103
Часы на контроль	45	45	45	45
Итого	180	180	180	180

Программу составил(и):
Ст.препод, Тарасенко Т.П.

Рабочая программа дисциплины
Управление корпоративной информационной безопасности

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 917)

составлена на основании учебного плана:
09.04.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Управление данными
утвержденного учебно-методическим советом вуза от 13.06.2024 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

Зав. кафедрой Лысенкова С.А., к.ф.-м.н., доцент

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения дисциплины является формирование базовых знаний в области информационной защиты телекоммуникационных и компьютерных систем и сетей на основе современных программных и операционных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Управление проектированием информационных систем
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Интеграция корпоративных систем
2.2.2	Выполнение и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-10.1: Демонстрирует знания по осуществлению общего контроля работы IT-кадров
ПК-10.2: Организовывает общий контроль работы IT-кадров
ПК-10.3: Контролирует работу IT-кадров
ПК-8.1: Демонстрирует знание методов развития и совершенствования сетей и инфокоммуникаций
ПК-8.2: Создает необходимое резервирование сетей и инфокоммуникаций
ПК-8.3: Обеспечивает бесперебойную работу сети
ПК-2.1: Демонстрирует знания теории баз данных и других хранилищ информации
ПК-2.2: Разрабатывает, вводит в действие и обслуживает базы данных и других хранилищ информации
ПК-2.3: Дополняет, модифицирует и совершенствует базы данных и другие хранилища информации
ПК-1.1: Демонстрирует знания моделей объектов профессиональной деятельности
ПК-1.2: Разрабатывает и исследует модели объектов профессиональной деятельности, предлагает и адаптирует методики, определяет качество проводимых исследований

ПК-1.3: Составляет отчеты о проделанной работе, обзоров, готовит публикации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	виды угроз для корпоративных информационных систем и методы обеспечения информационной безопасности корпоративных информационных систем, основные понятия и определения в области защиты информации; концепции и методы защиты информации; источники, риски и формы атак на информацию; стратегии аутентификации и авторизации; концепции сетевого аудита; технологии обнаружения вторжения; стратегии политик безопасности; принципы сетевой обороны.
3.2	**Уметь:**
3.2.1	выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в КИС, анализировать угрозы и факторы, влияющие на безопасность информации в компьютере, компьютерной системе и сети; создавать план защиты информационных объектов и их информационного взаимодействия; выбирать и применять обоснованное средство защиты; обновлять систему безопасности с использованием служб обновления, планировать политику безопасности объекта информатизации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Организация информационной защиты системы					
1.1	Организация информационной защиты корпоративной информационной системы /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.2	Организация информационной защиты корпоративной информационной системы /Ср/	3	9	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Основы криптографической защиты данных					
2.1	Симметричные и асимметричные криптосистемы /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

2.2	Симметричные и асимметричные алгоритмы /Лаб/	3	3,5	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.3	Симметричные и асимметричные криптосистемы /Ср/	3	9	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.4	Электронная цифровая подпись /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.5	Криптопровайдеры и шифрующие файловые системы /Лаб/	3	4,5	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.6	Криптопровайдеры и шифрующие файловые системы /Ср/	3	9	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.7	Системы управление ключевой информацией. /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.8	Изучение программных средств сканирования сетей и обнаружения атак /Лаб/	3	3,5	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

2.9	Изучение программных средств сканирования сетей и обнаружения атак /Ср/	3	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.10	Криптографические протоколы /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.11	Управление правами доступа пользователей/групп к информационным ресурсам /Лаб/	3	3,5	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.12	Криптографические протоколы /Ср/	3	11	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Защита доступа к информационным ресурсам корпоративной информационной системы					
3.1	Управление доступом к данным. /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
3.2	Управление доступом к данным. /Ср/	3	15	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. Безопасность удаленного доступа и межсетевого взаимодействия					

4.1	Методы защиты передачи данных в корпоративных информационных системах /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
4.2	Методы защиты передачи данных в корпоративных информационных системах /Ср/	3	15	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
4.3	Сетевые атаки /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
4.4	Сетевые атаки /Ср/	3	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 5. Защита системы от вредоносных программ					
5.1	Защита системы от вредоносных программ /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
5.2	Изучение антивирусных программных комплексов. /Лаб/	3	1	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
5.3	Защита системы от вредоносных программ /Ср/	3	15	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.4 Л1.5Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 6.					

6.1	/Контр.раб./	3	0	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
6.2	/Экзамен/	3	45	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлены отдельным документом

5.2. Оценочные материалы для диагностического тестирования

Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 2015, электронный ресурс	1
Л1.2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017, электронный ресурс	1
Л1.3	Шаньгин В.Ф.	Информационная безопасность и защита информации: учебное пособие	Саратов: Профобразование, 2017, электронный ресурс	1
Л1.4	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: Учебник	Москва: Издательство Юрайт, 2020, электронный ресурс	1
Л1.5	Эминов Б. Ф., Эминов Ф. И.	Корпоративные информационные системы: учебное пособие	Казань: КНИТУ-КАИ, 2019, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Мельников В. П., Клейменов С. А., Петраков А. М.	Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии"	М.: Академия, 2011	15
Л2.2	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2015, электронный ресурс	1
Л2.3	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018, электронный ресурс	1
Л2.4	Астапчук В. А., Терещенко П. В.	Корпоративные информационные системы: требования при проектировании: Учебное пособие	Москва: Издательство Юрайт, 2019, электронный ресурс	1
Л2.5	Баранова Е.К., Бабаш А.В.	?нформационная безопасность и защита информации: Учебное пособие	Москва: ?здательский Центр Р?О, 2019, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Левин М.	PGP: Кодирование и шифрование информации с открытым ключом	М.: Майор: Изд. А. И. Осипенко, 2001, электронный ресурс	1
Л3.2	Большаков А.С., Режеб Т.Б.К.	Методические указания и контрольные задания по дисциплине Инженерно-техническая защита информации: учебно-методическое пособие	Москва: Московский технический университет связи и информатики, 2013, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	российский общеобразовательный портал
Э2	электронный журнал Открытые системы
Э3	сайт Информационных технологий
Э4	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники.
Э5	журнал для ИТ-профессионалов.

6.3.1 Перечень программного обеспечения

6.3.1.1	Операционная система Windows
6.3.1.2	Пакет программ Microsoft Office

6.3.2 Перечень информационных справочных систем

6.3.2.1	Гарант-информационно-правовой портал. http://www.garant.ru/
6.3.2.2	КонсультантПлюс –надежная правовая поддержка. http://www.consultant.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Для проведения лекционных занятий необходима аудитория, оснащенная компьютером и мультимедийным оборудованием.
7.2	Для проведения лабораторных занятий необходим компьютерный класс, оборудованный техникой из расчета один компьютер на одного обучающегося, с обустроенным рабочим местом преподавателя.
7.3	Требуются персональные компьютеры с программным обеспечением MS OFFICE,локальная вычислительная сеть с выходом в глобальную сеть Internet.