Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 26.06.2025 07:02:25
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

11 июня 2025г., протокол УМС №5

Управление корпоративной информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план g090402-УпрДан-25-2.plx
09.04.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Управление данными

Квалификация **Магистр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 32
самостоятельная работа 40

Виды контроля в семестрах:
зачеты 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	17 2/6			
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	40	40	40	40
Итого	72	72	72	72

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

Рабочая программа дисциплины
Управление корпоративной информационной безопасностью

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 11.06.2025 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

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

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:	ФТД
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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
1.2	Организация информационной защиты корпоративной информационной системы /Ср/	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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Основы криптографической защиты					
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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.3	Симметричные и асимметричные криптосистемы /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	

2.6	Криптопровайдеры и шифрующие файловые системы /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	

2.9	Изучение программных средств сканирования сетей и обнаружения атак /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.12	Криптографические протоколы /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.2	Управление доступом к данным. /Ср/	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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.2	Методы защиты передачи данных в корпоративных информационных системах /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.4	Сетевые атаки /Ср/	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
5.3	Защита системы от вредоносных программ /Ср/	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 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.3 Э1 Э2 Э3 Э4 Э5	
6.2	/Зачёт/	3	25	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 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.4 Л3.2 Л3.3 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	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: Учебник	Москва: ?здательство Юрайт, 2020, электронный ресурс	1
Л1.2	Зенков А. В.	Информационная безопасность и защита информации: Учебное пособие для вузов	Москва: Юрайт, 2022, электронный ресурс	1
Л1.3	Эминов Б. Ф., Эминов Ф. И.	Корпоративные информационные системы: учебное пособие	Казань: КНИТУ-КАИ, 2019, электронный ресурс	1
Л1.4	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов	Москва: Юрайт, 2023, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Астапчук В. А., Терещенко П. В.	Корпоративные информационные системы: требования при проектировании: Учебное пособие	Москва: Издательство Юрайт, 2019, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2	Баранова Е.К., Бабаш А.В.	?нформационная безопасность и защита информации: Учебное пособие	Москва: ?здательский Центр Р?О?, 2019, электронный ресурс	1
Л2.3	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2020, электронный ресурс	1
Л2.4	Прохорова О. В.	Информационная безопасность и защита информации	Санкт-Петербург: Лань, 2021, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	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
Л3.2	Бахаров, Л. Е.	Информационная безопасность и защита информации: сборник тестов	Москва: Издательский Дом МИСиС, 2015, электронный ресурс	1
Л3.3	Бахаров, Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография): практикум	Москва: Издательский Дом МИСиС, 2019, электронный ресурс	1

Л3.4	Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А.	Информационная безопасность и защита информации: практикум	Дубна: Государственный университет «Дубна», 2020, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	российский общеобразовательный портал http://www.school.edu.ru
Э2	электронный журнал Открытые системы http://www.osp.ru
Э3	сайт Информационных технологий http://inftech.webservis.ru/
Э4	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники.http://www. computeiTa.ru
Э5	журнал для ИТ-профессионалов.http://www.bytemag.iTi/
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	учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (лабораторных занятий), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащена: комплект специализированной учебной мебели, маркерная (меловая) доска, комплект переносного мультимедийного оборудования - компьютер, проектор, проекционный экран, компьютеры с возможностью выхода в Интернет и доступом в электронную информационно-образовательную среду. Обеспечен доступ к сети Интернет и в электронную информационную среду организации.