

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 16.06.2025 13:33:28
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

Методы защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Автоматизированных систем обработки информации и управления		
Учебный план	b010302-ПМ-25-4.plx Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА Направленность (профиль): Прикладная математика и информатика		
Квалификация	бакалавр		
Форма обучения	очная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах: экзамены 7	
в том числе:			
аудиторные занятия	48		
самостоятельная работа	24		
часов на контроль	36		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
Неделя	17 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	16	16	16	16
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	24	24	24	24
Часы на контроль	36	36	36	36
Итого	108	108	108	108

Программу составил(и):

к.т.н., Доцент, Гавриленко Т.В.

Рабочая программа дисциплины

Методы защиты информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

Направленность (профиль): Прикладная математика и информатика

утвержденного учебно-методическим советом вуза от 11.06.2025 протокол № 5.

Рабочая программа одобрена на заседании кафедры

Автоматизированных систем обработки информации и управления

Зав. кафедрой Профессор каф. АСОИУ, д.т.н., Бушмелева К.И.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование знаний об основных положениях теории и практики информационной безопасности.
1.2	Умений применять современные методы и средства защиты информации в вычислительных системах и сетях.
1.3	Применять знания, методы математического анализа и моделирования, теоретического и экспериментального исследования для оценки рисков информационной безопасности и организации противодействия угрозам.
1.4	Использовать современные информационные технологии и программные средства, в том числе отечественного производства, для защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.03
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Системное программное обеспечение
2.1.2	Операционные системы
2.1.3	Программирование на СИ
2.1.4	Алгоритмы и методы программирования
2.1.5	Информатика
2.1.6	Основы программирования
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика, преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-4.1: Выполняет процедуры сборки программных модулей и компонент в программный продукт	
ПК-4.2: Проводит оценку работоспособности программного продукта	
ПК-3.1: Разрабатывает программное обеспечение, используя современные среды программирования	

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Базовый перечень методов и средств защиты компьютерной информации.
3.1.2	Различные способы сбора, обработки и представления информации на основе информационной и библиографической культуры с учетом современных требований информационной безопасности.
3.1.3	Состав и функциональные возможности современных информационных технологий и программных средств, в том числе отечественного производства, в части анализа, проектирования и разработки информационных и автоматизированных систем с учетом современных требований информационной безопасности.
3.1.4	Принципы классификации и примеры угроз безопасности компьютерным системам.
3.1.5	Методы использования знаний основ высшей математики, физики, инженерной графики, информатики, вычислительной техники, методов математического анализа, моделирования, программирования и проектирования, теоретического и экспериментального исследования в профессиональной деятельности.
3.1.6	Современные отечественные и международные стандарты информационной безопасности информационных систем.
3.2	Уметь:
3.2.1	Реализовывать методы криптографической защиты информации в вычислительных системах.
3.2.2	Использовать различные информационно-коммуникационные технологии для решения задач информационной безопасности на основе информационной и библиографической культуры.
3.2.3	Конфигурировать встроенные и дополнительные средства безопасности в операционной системе, локальных и глобальных сетях.

3.2.4	Выбирать и использовать современные информационные технологии и программные средства, в том числе отечественного производства, на всех стадиях жизненного цикла информационных и автоматизированных систем, при решении задач информационной безопасности.
3.2.5	Решать стандартные профессиональные задачи информационной безопасности с применением естественнонаучных и общеинженерных знаний.
3.2.6	Устанавливать и настраивать программное обеспечение для защиты компьютерной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Раздел 1					
1.1	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность защиты информации, связанной с составом и функциональными возможностями современных информационных технологий и программных средств. /Лек/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.2	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации. Изучение различных информационно-коммуникационные технологии и их уровней безопасности. Факторы повышения уязвимости систем на всех стадиях жизненного цикла информационных и автоматизированных систем. /Пр/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.3	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность защиты информации, связанной с составом и функциональными возможностями современных информационных технологий и программных средств. /Ср/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.4	Основные понятия информационной безопасности и их связь со знаниями основ высшей математики, физики, информатики, вычислительной техники. Защиты информации и разработка информационных и автоматизированных систем, при решении задач профессиональной деятельности. Информационная культура и информационная безопасность. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.5	Основные понятия информационной безопасности. Основные подходы к созданию моделей информационной безопасности. /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.6	Основные понятия информационной безопасности и их связь со знаниями основ высшей математики, физики, информатики, вычислительной техники. Защиты информации и разработка информационных и автоматизированных систем, при решении задач профессиональной деятельности. Информационная культура и информационная безопасность /Ср/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.7	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности. /Лек/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.8	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Применение информационных технологий и программных средств, в том числе отечественного производства, и законодательное регулирование их применения /Пр/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.9	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности.. /Ср/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.10	Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Лек/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.11	Информационные технологии и программные средства защиты информации /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.12	Проблемы защиты информации в АСОИУ. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Ср/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.13	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.14	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.15	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.16	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационные технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.17	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационные технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Пр/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.18	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационные технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.19	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.20	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.21	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.22	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Internet. /Лек/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.23	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Internet. /Пр/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.24	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Internet. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.25	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Лек/	7	4	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.26	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Пр/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.27	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.28	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.29	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.30	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.31	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Лек/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.32	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.33	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.34	Контрольная работа /Контр.раб./	7	0	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Выполнение контрольной работы
1.35	Экзамен /Экзамен/	7	36	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.4 Л1.2 Л1.3Л2.2 Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Устный опрос на зачете

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
--	---------------------	----------	-------------------	----------

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Суворова Г. М.	Информационная безопасность: Учебное пособие для вузов	Москва: Юрайт, 2021, электронный ресурс	1
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник для вузов	Санкт-Петербург: Лань, 2023, электронный ресурс	1
Л1.3	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2024, электронный ресурс	1
Л1.4	Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012, электронный ресурс	1
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Гулятьева Т. А.	Основы теории информации и криптографии: Конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, электронный ресурс	1
Л2.2	Братановский С. Н., Лапин С. Ю.	Обеспечение доступа граждан к информации о деятельности органов государственной власти и местного самоуправления в Российской Федерации. Информационно-правовой аспект: Монография	Саратов: Электронно-библиотечная система IPRbooks, 2012, электронный ресурс	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Башлы П. Н.	Информационная безопасность и защита информации	Москва: Издательский Центр РИО, 2013, электронный ресурс	1
Л3.2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017, электронный ресурс	1
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Журнал Успехи кибернетики https://ru.jcyb.ru/nisii_tech			
Э2	Журнал электронный журнал Открытые системы http://www.osp.ru			
Э3	Журнал о современных технологиях www.computerra.ru			
Э4	Вестник кибернетики https://www.vestcyber.ru/jour			
Э5	Журнал ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ https://www.aidt.ru/ru/			
6.3.1 Перечень программного обеспечения				
6.3.1.1	MS Office			

6.3.1.2	MS Visual Studio
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.
7.2	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.