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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

11 июня 2025 г., протокол УМС №5

МОДУЛЬ ДИСЦИПЛИН ПРОФИЛЬНОЙ НАПРАВЛЕННОСТИ
Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-ИнфСист-22-4.plx
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану	180	Виды контроля в семестрах:
в том числе:		экзамены 7
аудиторные занятия	64	
самостоятельная работа	80	
часов на контроль	36	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	80	80	80	80
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Программу составил(и):
старший преподаватель, Еловой Сергей Григорьевич

Рабочая программа дисциплины
Информационная безопасность и защита информации

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана:
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Информационные системы и технологии
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	формирование знаний об основных положениях теории и практики информационной безопасности; умений применять современные методы и средства защиты информации в вычислительных системах и сетях; компетенций в области разработки и использования средств защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах у студентов профиля подготовки – Вычислительные машины, комплексы, системы и сети.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Объектно-ориентированное программирование
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность баз данных

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-4.1: Демонстрирует знания методов и технологий обеспечения функционирования баз данных

ПК-4.2: Разрабатывает алгоритмы предотвращение потерь и повреждений данных

ПК-4.3: Обеспечивает информационную безопасность

ПК-11.1: Демонстрирует знания методов анализа требований к программному обеспечению

ПК-11.2: Применяет на практике методы организации работы по проектированию программного обеспечения

ПК-11.3: Проектирует программное обеспечение

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Математические основы криптографии, организационные, технические и программные методы защиты и анализа информации в современных компьютерных системах,сетях, програмного обеспечения, баз данных, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей, функционирования баз данных и проектированию програмного обеспечения;
3.2	**Уметь:**
3.2.1	Уметь применять известные, а также разарабатывать методы и средства поддержки информационной безопасности в компьютерных системах для предотвращения потерь и повреждений данных, при проектировании програмного обеспечения с соблюдением требований информационной безопасности.
3.3	**Владеть:**
3.3.1	Владеть навыками, методами и средствами защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи, установлении подлинности передаваемых сообщений, хранении информации (документов, баз данных), в том числе проектировать программное обеспечение со всеми требованиями для обеспечения информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Примечание**
	Раздел 1. Информационная безопасность. Основы.					
1.1	Информационная безопасность. Основы. /Лек/	7	2	ПК-4.1 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
1.2	Информационная безопасность. Основы. /Лаб/	7	3	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
1.3	Сравнение угроз /Ср/	7	10	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
	Раздел 2. Безопасность современных сетевых технологий.					
2.1	Безопасность современных сетевых технологий. /Лек/	7	4	ПК-4.1 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
2.2	Безопасность современных сетевых технологий. /Лаб/	7	4	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
2.3	Обзор публикаций по современных сетевых технологиям /Ср/	7	10	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
	Раздел 3. Методы обеспечения информационной безопасности информационных ресурсов.					
3.1	Методы обеспечения информационной безопасности информационных ресурсов. /Лек/	7	4	ПК-4.1 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
3.2	Методы обеспечения информационной безопасности информационных ресурсов. /Ср/	7	10	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
3.3	Методы обеспечения информационной безопасности информационных ресурсов. /Лаб/	7	4	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
	Раздел 4. Криптографические методы защиты информации					

4.1	Криптографические методы защиты информации /Лек/	7	12	ПК-4.1 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
4.2	Криптографические методы защиты информации /Лаб/	7	12	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
4.3	Прикладное использование криптографического ПО информации /Ср/	7	15	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
	Раздел 5. Методы и средства защиты информации в персональном компьютере и компьютерных сетях					
5.1	Методы и средства защиты информации в персональном компьютере и компьютерных сетях /Лек/	7	3	ПК-4.1 ПК-4.3 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
5.2	Методы и средства защиты информации в персональном компьютере и компьютерных сетях /Лаб/	7	4	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
5.3	Методы и средства защиты информации в персональном компьютере и компьютерных сетях /Ср/	7	12	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
	Раздел 6. Электронно-цифровая подпись					
6.1	Электронно-цифровая подпись /Лек/	7	4	ПК-4.1 ПК-11.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
6.2	Электронно-цифровая подпись /Лаб/	7	3	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
6.3	Электронно-цифровая подпись /Ср/	7	12	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
	Раздел 7. Инфраструктура открытых ключей					
7.1	Инфраструктура открытых ключей /Лек/	7	3	ПК-4.1 ПК-11.1 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	
7.2	Инфраструктура открытых ключей /Лаб/	7	2	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	

7.3	Инфраструктура открытых ключей /Ср/	7	11	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	
7.4	/Экзамен/	7	36	ПК-4.1 ПК-4.2 ПК-4.3 ПК-11.1 ПК-11.2 ПК-11.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Представлено отдельным документом

5.2. Темы письменных работ

Представлено отдельным документом

5.3. Фонд оценочных средств

Представлено 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	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
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	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РО, 2019, [Электронный ресурс]	1
Л1.5	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: Учебник	Москва: Издательство Юрайт, 2020, [Электронный ресурс]	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2015, [Электронный ресурс]	1
Л2.2	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 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

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

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	«Хабрахабр» [Электронный ресурс]. – 201-. – Режим доступа: http://habrahabr.ru/, свободный. – Загл. с экрана.
Э2	«SecurityLab» [Электронный ресурс]. – 201-. – Режим доступа: https://www.securitylab.ru/, свободный. – Загл. с экрана.

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	СПС «КонсультантПлюс» - www.consultant.ru/ СПС «Гарант» - www.garant.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.