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

ОСНОВЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ
Основы информационной безопасности
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-ИнфСист-25-1 Перезагрузка.plx
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 48
самостоятельная работа 69
часов на контроль 27

Виды контроля в семестрах:
экзамены 1

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		Итого	
Недель	17 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	69	69	69	69
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Программу составил(и):
Преподаватель, Воронцова Т.Д.;Преподаватель, Гончаров А.Р.

Рабочая программа дисциплины
Основы информационной безопасности

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 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; понимания основных концепций и принципов теории кодирования информации; умений анализировать и оптимизировать работу систем кодирования с учетом помех и ошибок передачи информации; умений анализировать и оценивать уровень защиты криптографических систем, и выбирать подходящие методы в зависимости от контекста использования у студентов

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.04.06
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика в объеме программы средней школы
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационные технологии
2.2.2	Технологии программирования
2.2.3	Разработка WEB-приложений

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

ОПК-3.1: Анализировать информационные ресурсы в Интернете и локальных базах данных для выбора релевантной информации для решения стандартных профессиональных задач

ОПК-3.2: Оценивать применение информационно-коммуникационных технологий для решения стандартных задач в профессиональной деятельности на основе информационной и библиографической культуры с учётом требований информационной безопасности

ОПК-3.3: Применять безопасные информационно-коммуникационные технологии для решения профессиональных задач

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основные понятия в области информационной безопасности; Современные методы и средства защиты информации в вычислительных системах и сетях; Основы криптографии и теории кодирования информации; Угрозы информационной безопасности и методы их предотвращения; Нормативные правовые акты, регулирующие вопросы безопасности информации; Математические основы криптографии, организационные, технические и программные методы защиты и анализа информации в современных компьютерных системах.
3.2	**Уметь:**
3.2.1	Разрабатывать и использовать средства защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах; Анализировать и оптимизировать работу систем кодирования с учетом помех и ошибок передачи информации; Оценивать уровень защиты криптографических систем и выбирать подходящие методы в зависимости от контекста использования; Совместно работать в группе для решения задач, связанных с обеспечением безопасности информационных систем и технологий.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Введение в информационную безопасность					

1.1	Основные понятия, цели и задачи информационной безопасности /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
1.2	Основные понятия, цели и задачи информационной безопасности /Лаб/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
1.3	Основные понятия, цели и задачи информационной безопасности /Ср/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
	Раздел 2. Угрозы и уязвимости информационных систем					
2.1	Классификация угроз и уязвимостей /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
2.2	Классификация угроз и уязвимостей /Лаб/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
2.3	Классификация угроз и уязвимостей /Ср/	1	5	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
2.4	Политики обеспечения безопасности. Модели управления доступом /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
2.5	Политики обеспечения безопасности. Модели управления доступом /Ср/	1	6	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
2.6	Политики обеспечения безопасности. Модели управления доступом /Лаб/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
	Раздел 3. Основы криптографии					
3.1	Симметричное и асимметричное шифрование. Электронная подпись, хэширование /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	

3.2	Симметричное и асимметричное шифрование. Электронная подпись, хэширование /Лаб/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
3.3	Симметричное и асимметричное шифрование. Электронная подпись, хэширование /Ср/	1	6	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
	Раздел 4. Методы идентификации, аутентификации и управления доступом					
4.1	Методы идентификации и аутентификации. Управление правами доступа /Лек/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
4.2	Методы идентификации и аутентификации. Управление правами доступа /Лаб/	1	4	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
4.3	Методы идентификации и аутентификации. Управление правами доступа /Ср/	1	8	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
	Раздел 5. Обеспечение информационной безопасности					
5.1	Методы анализа рисками и управление инцидентами /Лаб/	1	6	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
5.2	Методы анализа рисками и управление инцидентами /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
5.3	Методы анализа рисками и управление инцидентами /Ср/	1	20	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
5.4	Методы анализа рисками и управление инцидентами /Лек/	1	2	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	
5.5	Методы анализа рисками и управление инцидентами /Лаб/	1	6	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	

5.6	Методы анализа рисками и управление инцидентами /Ср/	1	20	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	Контрольная работа
5.7	/Экзамен/	1	27	ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Э1 Э2	

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	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов	Москва: Юрайт, 2023, электронный ресурс	1
Л1.2	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2023, электронный ресурс	1
Л1.3	Щербак А. В.	Информационная безопасность: учебник для вузов	Москва: Юрайт, 2025, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Сычев Ю. Н.	Защита информации и информационная безопасность: учебное пособие	Москва: ИНФРА-М, 2023, электронный ресурс	10
Л2.2	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов	Санкт-Петербург: Лань, 2024, электронный ресурс	1
Л2.3	Баранова Е.К., Бабаш А.В., Ларин Д.А.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИОИ, 2024, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2024, электронный ресурс	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Моргунов, А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019, электронный ресурс	1
Л3.2	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2024, электронный ресурс	1
Л3.3	Баланов А.Н.	Комплексная информационная безопасность: полный справочник специалиста: Практическое пособие	Вологда: Инфра-Инженерия, 2024, электронный ресурс	1
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	«SecurityLab» https://www.securitylab.ru/			
Э2	«The Hacker News» https://thehackernews.com/			
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/			
6.3.2.2	СПС «Гарант» - www.garant.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.
7.3	Обеспечен доступ к сети Интернет и в электронную информационную среду организации.