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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

15 июня 2023 г., протокол УМС №5

МОДУЛЬ ДИСЦИПЛИН ПРОФИЛЬНОЙ НАПРАВЛЕННОСТИ
Основы информационной безопасности
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-БезопИнфСист-23-1.plx
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Безопасность информационных систем и технологий

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 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
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.

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): Безопасность информационных систем и технологий
утвержденного учебно-методическим советом вуза от 15.06.2023 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

Зав. кафедрой к.т.н. доцент Федоров Д.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; 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 профиля подготовки – Безопасность информационных систем и технологий

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	Основы программирования
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность баз данных
2.2.2	Криптографические методы защиты информации
2.2.3	Сети ЭВМ

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-4. Способен выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности
ПК-4.3: Обеспечивает информационную безопасность

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.
3.3	**Владеть:**
3.3.1	Навыками анализа уязвимости информационных систем и разработки плана мер по обеспечению их безопасности; Навыками оценки рисков, связанных с использованием информационных систем и технологий, и разработки плана их минимизации; Навыками сравнения, выбора и использования средств защиты информации в зависимости от задач и условий их применения; Навыками анализа и тестирования систем защиты информации с целью определения их эффективности и обеспечения их надежности; методами и средствами защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи, установлении подлинности автора передаваемых сообщений.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Примечание**
	Раздел 1. Понятие информационной безопасности					

1.1	Основные понятия информационной безопасности. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
1.2	Организационно-правовая база. /Лек/	1	4	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
	Раздел 2. Основы теории кодирования					
2.1	Моделирование источников сообщений и каналов связи. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.2	Моделирование источников сообщений и каналов связи. /Лаб/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.3	Моделирование источников сообщений и каналов связи. /Ср/	1	6		Э2	
2.4	Понятие кодирования /Лек/	1	4	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.5	Понятие кодирования /Ср/	1	6		Э2	
2.6	Понятие кодирования /Лаб/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.7	Сжимающие коды. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.8	Помехоустойчивые коды. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.9	Практика кодирования /Лаб/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
2.10	Практика кодирования /Ср/	1	6	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
	Раздел 3. Защита конфиденциальности					
3.1	История криптографии. /Лек/	1	4	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
3.2	Практика шифрования и криптоанализа /Лаб/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
3.3	Практика шифрования и криптоанализа /Ср/	1	6	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
3.4	Современные шифрсистемы. /Лек/	1	4	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	

3.5	Современные шифрсистемы. /Лаб/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
3.6	Современные шифрсистемы. /Ср/	1	6	ПК-4.3	Л1.1Л2.1Л3.1 Э2	
3.7	Стеганогрфия. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
	Раздел 4. Защита доступности					
4.1	Сетевые технологии /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
4.2	Системы разграничения прав доступа. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
4.3	Протоколы ААА. /Лек/	1	2	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
	Раздел 5. Работа над проектом					
5.1	Самостоятельная работа над проектом /Лаб/	1	6	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
5.2	Самостоятельная работа над проектом /Ср/	1	39	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
5.3	/Контр.раб./	1	13	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	
5.4	/Экзамен/	1	14	ПК-4.3	Л1.1 Л1.2Л2.1Л3.1 Э2	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлено в приложении

5.2. Оценочные материалы для диагностического тестирования

Представлено в приложении

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	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2023, Электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.2	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	Сычев Ю. Н.	Защита информации и информационная безопасность: учебное пособие	Москва: ИНФРА-М, 2023	10
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

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 «КонсультантПлюс» - 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.