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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

13 июня 2024г., протокол УМС №5

Прикладная криптография

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-ИнфСист-24-2.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 32
самостоятельная работа 85
часов на контроль 27

Виды контроля в семестрах:
экзамены 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		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	85	85	85	85
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Программу составил(и):

Рабочая программа дисциплины

Прикладная криптография

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 13.06.2024 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	Цель курса – подготовка студентов к использованию и интеграции в информационных системах и базах данных, систем шифрования и защиты данных, формирование знаний об основных принципах защиты данных и шифрования, формирование навыков использования некоторых известных систем шифрования в различных видах информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационные технологии
2.1.2	Алгоритмы и языки программирования
2.1.3	Информатика
2.1.4	Основы информационной безопасности
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	Безопасность баз данных
2.2.3	Производственная практика, преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-2.1: Демонстрирует знания методов, алгоритмов и технологий интеграции программных модулей и компонент
ПК-2.2: Применяет на практике методы, алгоритмы и технологии интеграции программных модулей и компонент
ПК-2.3: Владеет технологиями интеграции программных модулей и компонент
ПК-4.1: Демонстрирует знания методов и технологий обеспечения функционирования баз данных
ПК-4.2: Разрабатывает алгоритмы предотвращения потерь и повреждений данных
ПК-4.3: Обеспечивает информационную безопасность
ПК-5.1: Демонстрирует знания этапов, методов и технологий по созданию (модификации) информационных систем
ПК-5.2: Разрабатывает и модифицирует информационные системы
ПК-5.3: Сопровождает информационные системы
ПК-16.1: Демонстрирует знания методов анализа защищенности информационных систем

ПК-16.2: Применяет на практике методы проведения анализа защищенности информационных систем

ПК-16.3: Проводит анализ защищенности информационных систем

ПК-17.1: Демонстрирует знания методов организации разработки, внедрения, и сопровождения информационной системы с учетом требование информационной безопасности

ПК-17.2: Применяет на практике методы организации разработки, внедрения, и сопровождения информационной системы с учетом требование информационной безопасности

ПК-17.3: Выполняет разработку, внедрение, и сопровождение информационной системы с учетом требование информационной безопасности	
Знать:	
Уровень 1	.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	основные направления развития криптографии, теории информации и
3.1.2	теории кодирования;
3.1.3	основные принципы построения кодов, криптосистем и крипто протоколов;
3.1.4	основные методы анализа криптостойкости информационных систем;
3.1.5	основные алгоритмы шифрования;
3.1.6	основные протоколы защищенной передачи данных.
3.2	**Уметь:**
3.2.1	конструировать криптостойкие алгоритмы и протоколы;
3.2.2	проводить анализ криптостойкости алгоритмы и протоколов;
3.2.3	создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1.					
1.1	Основные понятия криптографии /Лек/	4	1	ПК-4.1 ПК-16.1 ПК-17.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
1.2	Основные понятия криптографии /Лаб/	4	1	ПК-4.3 ПК-16.3 ПК-17.3 ПК-2.1 ПК-2.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	

1.3	Основные понятия криптографии /Ср/	4	8	ПК-4.3 ПК-16.3 ПК-17.3 ПК-2.1 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 2.					
2.1	Симметричное шифрование. /Лек/	4	4	ПК-4.1 ПК-16.1 ПК-17.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.2	Симметричное шифрование. /Лаб/	4	4	ПК-4.2 ПК-16.2 ПК-17.2 ПК-2.1 ПК-2.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.3	Симметричное шифрование. /Ср/	4	16	ПК-4.2 ПК-4.3 ПК-16.1 ПК-17.1 ПК-2.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 3.					
3.1	Ассиметричное шифрование. /Лек/	4	4	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.2	Ассиметричное шифрование. /Лаб/	4	4	ПК-4.2 ПК-2.1 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.3	Ассиметричное шифрование. /Ср/	4	15	ПК-4.3 ПК-2.1 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 4.					

4.1	Проблемы передачи информации. /Лек/	4	4	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.2	Проблемы передачи информации. /Лаб/	4	4	ПК-2.1 ПК-2.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.3	Проблемы передачи информации. /Ср/	4	18	ПК-4.3 ПК-2.1 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 5.					
5.1	Стеганография /Лек/	4	2	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
5.2	Стеганография /Лаб/	4	2	ПК-4.2 ПК-2.1 ПК-2.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
5.3	Стеганография /Ср/	4	14	ПК-4.3 ПК-16.3 ПК-17.2 ПК-2.1 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 6.					
6.1	Основы криптоанализа /Лек/	4	1	ПК-4.1 ПК-16.3 ПК-17.2 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
6.2	Основы криптоанализа /Лаб/	4	1	ПК-4.2 ПК-2.1 ПК-2.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	

6.3	Основы криптоанализа /Ср/	4	14	ПК-4.3 ПК-17.1 ПК-2.1 ПК-2.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
6.4	/Контр.раб./	4	0	ПК-4.1 ПК-4.2 ПК-4.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3	Э1 Э2 Э3 Э4 Э5	
	Раздел 7.					
7.1	/Экзамен/	4	27	ПК-4.1 ПК-4.2 ПК-4.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Сдача экзамена.

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	Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2023, электронный ресурс	1
Л1.2	Фомичёв В. М., Мельников Д. А.	Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов	Москва: Юрайт, 2024, электронный ресурс	1
Л1.3	Васильева И. Н.	Криптографические методы защиты информации: учебник и практикум для вузов	Москва: Юрайт, 2024, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.4	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов	Москва: Юрайт, 2024, электронный ресурс	1
Л1.5	Фомичёв В. М., Мельников Д. А.	Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов	Москва: Юрайт, 2024, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Креопалов В. В.	Технические средства и методы защиты информации: Учебное пособие	Москва: Евразийский открытый институт, 2011, электронный ресурс	1
Л2.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, электронный ресурс	1
Л2.3	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	Левин М.	PGP: Кодирование и шифрование информации с открытым ключом	М.: Майор: Изд. А. И. Осипенко, 2001	1
Л3.2	Ермакова А. Ю.	Криптографические методы защиты информации: учебно-методическое пособие	Москва: РТУ МИРЭА, 2021, электронный ресурс	1
Л3.3	Никулин В. В.	Безопасность и защита информации. Лабораторный практикум: учебно-методическое пособие для студентов направления подготовки 09.04.03 прикладная информатика	Брянск: Брянский ГАУ, 2021, 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.school.edu.ru

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет прикладных программ Microsoft Office
6.3.1.2	Операционная система Windows

6.3.2 Перечень информационных справочных систем

6.3.2.1	http://www.garant.ru Информационно-правовой портал Гарант.ру
6.3.2.2	http://www.consultant.ru/ Справочно-правовая система Консультант Плюс

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