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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

16 июня 2022 г., протокол УС №6

Прикладная криптография

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 32
самостоятельная работа 40
часов на контроль 36

Виды контроля в семестрах:
экзамены 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	10			
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	40	40	40	40
Часы на контроль	36	36	36	36
Итого	108	108	108	108

Программу составил(и):
Доцент, Федоров Д.А.

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): Информационные системы и технологии
утвержденного учебно-методическим советом вуза от 16.06.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

Зав. кафедрой к.т.н., Д. А. Фёдоров

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.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационная безопасность и защита информации
2.1.2	Методы защиты информации
2.1.3	Организационное и правовое обеспечение 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 интеграция программных модулей и компонент
ПК-2.2: Применяет на практике методы, алгоритмы и технологии интеграция 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 предотвращение 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

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;
3.3	**Владеть:**
3.3.1	навыком построения криптостойких алгоритмов шифрования и протоколов
3.3.2	передачи данных;
3.3.3	методами и формами защиты информации програмных модулей,информационных систем 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.					
1.1	Основные понятия криптографии /Лек/	8	1	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
1.2	Основные понятия криптографии /Лаб/	8	1	ПК-4.3 ПК-5.3	Л1.1 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Э1 Э2 Э3 Э4 Э5	
1.3	Основные понятия криптографии /Ср/	8	3	ПК-4.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 2.					
2.1	Симметричное шифрование. /Лек/	8	4	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.2	Симметричное шифрование. /Лаб/	8	4	ПК-4.2 ПК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5	

2.3	Симметричное шифрование. /Ср/	8	8	ПК-4.2 ПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 3.					
3.1	Ассиметричное шифрование. /Лек/	8	4	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.2	Ассиметричное шифрование. /Лаб/	8	4	ПК-4.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.3	Ассиметричное шифрование. /Ср/	8	10	ПК-4.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 4.					
4.1	Проблемы передачи информации. /Лек/	8	4	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.2	Проблемы передачи информации. /Лаб/	8	4	ПК-2.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.3	Проблемы передачи информации. /Ср/	8	9	ПК-4.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 5.					

5.1	Стеганография /Лек/	8	2	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
5.2	Стеганография /Лаб/	8	2	ПК-4.2 ПК-2.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
5.3	Стеганография /Ср/	8	5	ПК-4.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 6.					
6.1	Основы криптоанализа /Лек/	8	1	ПК-4.1 ПК-2.1 ПК-5.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
6.2	Основы криптоанализа /Лаб/	8	1	ПК-4.2 ПК-2.2 ПК-5.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
6.3	Основы криптоанализа /Ср/	8	5	ПК-4.3 ПК-2.3 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 7.					
7.1	/Экзамен/	8	36	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Итоговая контрольная работа. Сдача экзамена.

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	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017, [Электронный ресурс]	1
Л1.2	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017, [Электронный ресурс]	1
Л1.3	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018, [Электронный ресурс]	1
Л1.4	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
Л2.1	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
Л2.2	Креопалов В. В.	Технические средства и методы защиты информации: Учебное пособие	Москва: Евразийский открытый институт, 2011, [Электронный ресурс]	1
Л2.3	Васильков А. В., Васильков И. А.	Безопасность и управление доступом в информационных системах: учебное пособие	Москва: Издательство "ФОРУМ", 2017, [Электронный ресурс]	1
Л2.4	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РО 2019, [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

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.2	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2015, [Электронный ресурс]	1
Л3.3	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 2015, [Электронный ресурс]	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	российский общеобразовательный портал
Э2	электронный журнал Открытые системы
Э3	сайт Информационных технологий
Э4	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники.
Э5	журнал для ИТ-профессионалов.
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	СПС «КонсультантПлюс» - www.consultant.ru/ СПС «Гарант» - www.garant.ru/
6.3.2.2	http://www.consultant.ru/ Справочно-правовая система Консультант Плюс

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	аудитория, оборудованная техническими средствами для демонстрации лекций-визуализаций;
7.2	лабораторные работы должны выполняться в специализированных классах, оснащенных современными персональными компьютерами, включенными в сеть и программным обеспечением, в соответствии с тематикой изучаемого материала;
7.3	число рабочих мест в классах должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере;