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

Криптографические методы защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-БезопИнфСист-23-3.plx
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Безопасность информационных систем и технологий

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 64
самостоятельная работа 44

Виды контроля в семестрах:
зачеты 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		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	44	44	44	44
Итого	108	108	108	108

Программу составил(и):
Ст. преподаватель, Григоренко Виолетта Вячеславовна;Преподаватель, Воронцова Татьяна Дмитриевна

Рабочая программа дисциплины
Криптографические методы защиты 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): 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 Федеров Дмитрий Алексеевич

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; понимание принципов криптографии и ее роли в защите информации; изучение основных алгоритмов и протоколов криптографии; овладение навыками выбора и применения подходящих криптографических методов в различных сценариях; формирование способности анализировать уязвимости и потенциальные атаки на криптографические системы; освоение методов проверки и аудита криптографической безопасности; понимание этических, юридических и социальных аспектов применения криптографии 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	Сети ЭВМ
2.1.2	Теория информационных процессов и систем
2.1.3	Информатика
2.1.4	Сети ЭВМ
2.1.5	Теория информационных процессов и систем
2.1.6	Информатика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность информационных систем
2.2.2	Управление информационной безопасностью
2.2.3	Информационная безопасность и защита информации
2.2.4	Безопасность баз данных
2.2.5	Управление информационной безопасностью
2.2.6	Информационная безопасность и защита информации
2.2.7	Безопасность информационных систем
2.2.8	Безопасность баз данных

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1.1: Демонстрирует знания основных методов, моделей и алгоритмов исследования информационных систем и технологий.
ПК-1.2: Осуществляет выбор методов, моделей исследования информационных систем
ПК-1.3: Владеет технологиями исследования и моделирования информационных систем
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-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

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основные принципы информационной безопасности. Основные принципы криптографии, алгоритмы и протоколы. Математические основы криптографических алгоритмов. Уязвимости и атаки на криптографические системы. Международные нормы и стандарты криптографии.
3.2	**Уметь:**
3.2.1	Применять криптографические алгоритмы и протоколы для защиты информации в соответствии с потребностями и ограничениями. Анализировать и оценивать криптографическую безопасность систем. Анализировать этические, юридические и социальные аспекты применения криптографии.
3.3	**Владеть:**
3.3.1	Навыками разработки и реализации криптографических протоколов и систем; оценки уровня защиты информации и необходимости криптографических мер безопасности; научных исследований и разработок в области криптографии и защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Ведение в криптинрафию					
1.1	История криптографии. Стойкость преобразований. Уязвимости и криптоанализ. /Лек/	5	10	ПК-1.1 ПК-1.2 ПК-1.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2	
1.2	Частотный криптоанализ. Метод Касиски. /Лаб/	5	4	ПК-1.1 ПК-1.2 ПК-1.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2	
1.3	История криптографии. Стойкость преобразований. Уязвимости и криптоанализ. /Ср/	5	8	ПК-1.1 ПК-1.2 ПК-1.3	Л1.2Л2.1Л3.2 Э1 Э2	
	Раздел 2. Математические основы криптографии					
2.1	Основы теории чисел. Модульная арифметика. Основы теории групп, колец и полей. /Лек/	5	8	ПК-1.2 ПК-1.3	Л1.2Л2.1Л3.2 Э1 Э2	
2.2	Линейные преобразования и матрицы. Алгебраическая модель шифра. /Лаб/	5	6	ПК-1.2 ПК-1.3	Л1.2Л2.1Л3.2 Э1 Э2	
2.3	Основы теории чисел. Модульная арифметика. Основы теории групп, колец и полей. /Ср/	5	8	ПК-1.2 ПК-1.3	Л1.2Л2.1Л3.2 Э1 Э2	
	Раздел 3. Протоколы					

3.1	Асимметричное шифрование. ГОСТы симметричного шифрования.DES и AES. /Лек/	5	8	ПК-4.1 ПК-4.2 ПК-4.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
3.2	Протоколы генерации сеансовых ключей. Разделение секрета. Схема Блома. Сети Фейстеля и SP-сети. Хэширование и ЭЦП. /Лаб/	5	10	ПК-4.1 ПК-4.2 ПК-4.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
3.3	Асимметричное шифрование. ГОСТы симметричного шифрования.DES и AES. /Ср/	5	8	ПК-4.1 ПК-4.2 ПК-4.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
	Раздел 4. Аутентификация					
4.1	Протоколы безопасного обмена информацией (SSL/TLS, SSH). Протоколы аутентификации (Kerberos, OAuth, OpenID). Протоколы защиты интернета вещей (IoT). /Лек/	5	6	ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
4.2	Протоколы безопасного обмена информацией (SSL/TLS, SSH). Протоколы аутентификации (Kerberos, OAuth, OpenID). Протоколы защиты интернета вещей (IoT). /Ср/	5	8	ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
	Раздел 5. Работа над проектом					
5.1	Самостоятельная работа над проектом /Лаб/	5	12	ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
5.2	Самостоятельная работа над проектом /Ср/	5	12	ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 Э1 Э2	
	Раздел 6. Зачет					
6.1	Зачет /Зачёт/	5	0	ПК-1.1 ПК-1.2 ПК-1.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.2Л2.1Л3.2 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	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2019, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.2	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2020, электронный ресурс	1
Л1.3	Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А.	Информационная безопасность и защита информации: практикум	Дубна: Государственный университет «Дубна», 2020, электронный ресурс	1
Л1.4	Алекперов И. Д., Храмов В. В., Горбачева А. А., Фомичев Д. С.	Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учебное пособие	Ростов-на-Дону: ИУБиП, 2020, электронный ресурс	1
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Жук А.П., Жук Е.П.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2021, электронный ресурс	1
Л2.2	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2021, электронный ресурс	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Зенков А. В.	Информационная безопасность и защита информации: Учебное пособие для вузов	Москва: Юрайт, 2021, электронный ресурс	1
Л3.2	Степанова Е. А., Елизаров А. А., Шилер А. В.	Программно-аппаратные средства противодействия техническим разведкам на железнодорожном транспорте: учебно-методическое пособие к выполнению лабораторных работ	Омск: ОмГУПС, 2020, электронный ресурс	1
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	«SecurityLab»			
Э2	«Enigma Simulator»			
6.3.1 Перечень программного обеспечения				
6.3.1.1	Операционная система Windows, Пакет программ Microsoft Office бесрочно			
6.3.2 Перечень информационных справочных систем				
6.3.2.1	СПС «КонсультантПлюс», СПС «Гарант»			

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. Требуются персональные компьютеры с программным обеспечением MS OFFICE, пакет прикладных программ для статистического анализа данных SPSS или Statistica (версия не ниже 8), локальная вычислительная сеть с выходом в глобальную сеть Internet.