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

МОДУЛЬ ДИСЦИПЛИН ПРОФИЛЬНОЙ НАПРАВЛЕННОСТИ
Программно-аппаратные средства обеспечения информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-БезопИнфСист-25-3.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 51
часов на контроль 45

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	17 2/6			
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	51	51	51	51
Часы на контроль	45	45	45	45
Итого	144	144	144	144

Программу составил(и):
канд.физ.-мат.наук., Доцент, Берестин Д.К.

Рабочая программа дисциплины
Программно-аппаратные средства обеспечения 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 11.06.2025 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

Зав. кафедрой канд. физ.-мат. наук, доцент, Лысенкова С.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения учебной дисциплины является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационные технологии
2.1.2	Технология программирования
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационная безопасность и защита информации
2.2.2	Корпоративные информационные системы

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-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-7.1: Демонстрирует знания методов управления программно-аппаратными средствами инфокоммуникационной системы организации

ПК-7.2: Управляет программно-аппаратными средствами инфокоммуникационной системы организации

ПК-7.3: Выполняет администрирование сетей

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

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	базовый понятийный аппарат в области информационной безопасности;
3.1.2	функционирование системы управления средствами безопасности;
3.1.3	основные типы моделей управления доступом.
3.2	**Уметь:**
3.2.1	классифицировать информацию с ограниченным доступом применительно к видам тайны;
3.2.2	грамотно применять методы криптографической защиты;
3.2.3	применять системы управления средствами безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Примечание**
	Раздел 1. Раздел 1.					
1.1	Тема 1. Предмет и задачи программно- аппаратной защиты информации /Лек/	6	2	ПК-1.2 ПК-7.2 ПК-17.3 ПК-16.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.2	Тема 1. Предмет и задачи программно- аппаратной защиты информации /Лаб/	6	1	ПК-1.3 ПК-7.2 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.3	Тема 1. Предмет и задачи программно- аппаратной защиты информации /Ср/	6	5	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.4	Тема 2. Программно-аппаратные средства защиты информации /Лек/	6	2	ПК-1.1 ПК-1.3 ПК-5.3 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.5	Тема 2. Программно-аппаратные средства защиты информации /Лаб/	6	1	ПК-5.3 ПК-7.2 ПК-17.3 ПК-16.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.6	Тема 2. Программно-аппаратные средства защиты информации /Ср/	6	5	ПК-5.3 ПК-7.2 ПК-17.3 ПК-16.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.7	Тема 3. Контроль доступа к файлам /Лек/	6	4	ПК-1.2 ПК-5.1 ПК-7.1 ПК-17.3 ПК -16.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.8	Тема 3. Контроль доступа к файлам /Лаб/	6	2	ПК-17.3 ПК -16.1 ПК-16.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
1.9	Тема 3. Контроль доступа к файлам /Ср/	6	5	ПК-7.1 ПК-7.3 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
	Раздел 2. Раздел 2.					

2.1	Тема 1. Электронная цифровая подпись (ЭЦП) /Лек/	6	4	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.2	Тема 1. Электронная цифровая подпись (ЭЦП) /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.3	Тема 1. Электронная цифровая подпись (ЭЦП) /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.4	Тема 2. Программно-аппаратные средства шифрования /Лек/	6	4	ПК-1.1 ПК-5.1 ПК-7.2 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.5	Тема 2. Программно-аппаратные средства шифрования /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.6	Тема 2. Программно-аппаратные средства шифрования /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.7	Тема 3. Методы и средства ограничения доступа /Лек/	6	4	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.8	Тема 3. Методы и средства ограничения доступа /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
2.9	Тема 3. Методы и средства ограничения доступа /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
	Раздел 3. Раздел 3.					

3.1	Тема 1. Защита программ /Лек/	6	4	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.2	Тема 1. Защита программ /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.3	Тема 1. Защита программ /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.4	Тема 2. Защита от разрушающих программных воздействий (РПВ) /Лек/	6	4	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.5	Тема 2. Защита от разрушающих программных воздействий (РПВ) /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.6	Тема 2. Защита от разрушающих программных воздействий (РПВ) /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.7	Тема 3. Средства предотвращения утечки информации по техническим каналам /Лек/	6	4	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.8	Тема 3. Средства предотвращения утечки информации по техническим каналам /Лаб/	6	2	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
3.9	Тема 3. Средства предотвращения утечки информации по техническим каналам /Ср/	6	6	ПК-1.1 ПК-1.2 ПК-5.1 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	

3.10	/Контр.раб./	6	0	ПК-1.1 ПК-1.2 ПК-1.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК-17.1 ПК-17.2 ПК-17.3 ПК-16.1 ПК-16.2 ПК-16.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2	
	Раздел 4. Итоговый контроль					
4.1	/Экзамен/	6	45	ПК-1.1 ПК-1.2 ПК-1.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК-17.1 ПК-17.2 ПК-17.3 ПК-16.1 ПК-16.2 ПК-16.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 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	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: Учебник и практикум для вузов	Москва: Юрайт, 2022, электронный ресурс	1
Л1.2	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов	Москва: Юрайт, 2023, электронный ресурс	1
Л1.3	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов	Москва: Юрайт, 2025, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Гриднев, В. А., Губсков, Ю. А., Дерябин, А. С., Яковлев, А. В.	Программно-аппаратные средства защиты информации. В 3 частях. Ч.1: учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2022, электронный ресурс	1
Л2.2	Булычёв Г. Г.	Программно-аппаратные средства защиты информации. Часть 2	Москва: РТУ МИРЭА, 2022, электронный ресурс	1

Л2.3	Булычёв Г. Г.	Программно-аппаратные средства защиты информации. Часть 1	Москва: РТУ МИРЭА, 2022, электронный ресурс	1
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4	Гриднев, В. А., Губсков, Ю. А., Дерябин, А. С., Яковлев, А. В.	Программно-аппаратные средства защиты информации. В 3 частях. Ч.2: учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023, электронный ресурс	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Фомин, Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум	Саратов: Вузовское образование, 2021, электронный ресурс	1
Л3.2	Фомин, Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум	Саратов: Вузовское образование, 2021, электронный ресурс	1
Л3.3	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
Л3.4	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности.Часть 1: Методические рекомендации	Москва: РТУ МИРЭА, 2020, электронный ресурс	1
Л3.5	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности. Часть 2	Москва: РТУ МИРЭА, 2020, электронный ресурс	1
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	SecurityLabhttps://www.securitylab.ru/			
Э2	Хабрахабрhttp://habrahabr.ru/			
6.3.1 Перечень программного обеспечения				
6.3.1.1	Операционная система Microsoft. Пакет прикладных программ Microsoft Office. Интерпретатор языка Python 2.7 и выше, компилятор MinGW 4 и выше, среда разработки Microsoft Visual Studio, Visual Studio Code.			
6.3.2 Перечень информационных справочных систем				
6.3.2.1	Гарант-информационно-правовой портал. http://www.garant.ru/			
6.3.2.2	КонсультантПлюс –надежная правовая поддержка. http://www.consultant.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.