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

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

11 июня 2025 г., протокол УМС №5

Безопасность информационных систем

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 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	17 1/6			
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):
Преподаватель, Воронцова Татьяна Дмитриевна;Ст. преподаватель, Григоренко Виолетта Вячеславовна

Рабочая программа дисциплины
Безопасность информационных систем

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 к.ф.-м..н., доцент Лысенкова С.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Изучение принципов проектирования и анализа защищенности информационных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Рзаработка и эксплуатация защишенных информационных систем
2.1.2	Теория информационных процессов и систем
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	Программно-аппаратные-средства обеспечения информационной безопасностью
2.2.3	Надежность информационных систем
2.2.4	Качество информационных систем
2.2.5	Безопасность баз данных

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
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	Методы организации разработки, внедрения и сопровождения информационной системы с учетом требование информационной безопасности. Методов анализа защищенности информационных систем. Методов управления программно-аппаратными средствами инфокоммуникационной системы организации. Этапы, методы и технологий по созданию (модификации) информационных систем
3.2	**Уметь:**
3.2.1	Применять на практике методы организации разработки, внедрения, и сопровождения информационной системы с учетом требование информационной безопасности. Применять на практике методы проведения анализа защищенности информационных систем. Управлять программно-аппаратными средствами инфокоммуникационной системы организации. Разрабатывать и модифицировать информационные системы.
3.3	**Владеть:**
3.3.1	Технологией разработки, внедрения, и сопровождения информационной системы с учетом требование информационной безопасности. Технологией анализа защищенности информационных систем. Технологией администрирования сетей. Технологией сопровождения информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Обзор стандартов информационных систем					
1.1	Обзор стандартов информационных систем /Лек/	6	8	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.2	ISO/ IEC 27000 Использование антивирусных программ /Лаб/	6	8	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.3	Обзор стандартов информационных систем /Ср/	6	5	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 2. Уязвимости информационных систем					

2.1	Уязвимости информационных систем /Ср/	6	5	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.2	Уязвимости информационных систем /Лек/	6	8	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.3	Сканирование уязвимостей информационной системы. Сетевые вирусы. /Лаб/	6	6	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 3. Атаки информационных систем					
3.1	Атаки информационных систем /Лек/	6	8	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.2	Атаки отказ в обслуживании. /Лаб/	6	6	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.3	Атаки информационных систем /Ср/	6	5	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 4. Обеспечение информационной безопасности в информационных системах					
4.1	Обеспечение информационной безопасности в информационных системах /Лек/	6	4	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК- 16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

4.2	Создания защищенных средств связи объектов на основе стандартов ISO 7498-2, 17799, 15408. Разработка политики и правил информационной безопасности /Лаб/	6	4	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.3	Обеспечение информационной безопасности в информационных системах /Ср/	6	5	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 5. Управление информационной безопасностью в организации					
5.1	Разработка стратегии информационной безопасности. Управление проектами безопасности. /Лек/	6	4	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
5.2	Планирование и управление проектами безопасности. /Лаб/	6	4	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
5.3	Разработка стратегии информационной безопасности. Управление проектами безопасности. Планирование и управление проектами безопасности. /Ср/	6	5	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 6. Работа над проектом					
6.1	Самостоятельная работа над проектом. /Лаб/	6	4	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
6.2	Самостоятельная работа над проектом. /Ср/	6	19	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 7. Зачет					
7.1	Зачет /Зачёт/	6	0	ПК-5.1 ПК- 5.2 ПК- 5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК- 16.1 ПК-16.2 ПК- 16.3 ПК- 17.1 ПК-17.2 ПК- 17.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

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	Башлы П. Н., Бабаш А. В., Баранова Е. К.	Информационная безопасность и защита информации: Учебное пособие	Москва: Евразийский открытый институт, 2012, Электронный ресурс	1
Л1.2	Золотарев В. В.	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010, Электронный ресурс	1
Л1.3	Жукова М. Н.	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012, Электронный ресурс	1
Л1.4	Анисимов А. А.	Менеджмент в сфере информационной безопасности: Учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, Электронный ресурс	1
Л1.5	Баранова Е.К., Бабаш А.В.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИОР, 2020, Электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Шилов А.К.	Управление информационной безопасностью: Учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2018, Электронный ресурс	1
Л2.2	Партыка Т. Л., Попов И.И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2021, Электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Фомин Д. В.	Информационная безопасность: Учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика»	Саратов: Вузовское образование, 2018, Электронный ресурс	1
Л3.2	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2021, Электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	«SecurityLab»
Э2	«WebGoat»
Э3	«Damn Vulnerable Web Application»
Э4	«OWASP Juice Shop»

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.
7.3	Требуются персональные компьютеры с программным обеспечением MS OFFICE,локальная вычислительная сеть с выходом в глобальную сеть Internet.