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

Разработка и эксплуатация защищенных информационных систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики и вычислительной техники**

Учебный план b090302-БезопИнфСист-23-1.plx
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
Направленность (профиль): Безопасность информационных систем и технологий

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 32
самостоятельная работа 40

Виды контроля в семестрах:
зачеты 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	40	40	40	40
Итого	72	72	72	72

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

Рабочая программа дисциплины
Разработка и эксплуатация защищенных 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 15.06.2023 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Информатики и вычислительной техники

Зав. кафедрой к.т.н., доцент Федоров 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; компетенций в области разработки и использования средств защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах; овладение методами и технологиями разработки защищенных информационных систем; получение навыков в области анализа уязвимостей и рисков в информационных системах, а также разработки мер по их устранению; понимание принципов управления доступом к информационным ресурсам и методов аутентификации и авторизации пользователей у студентов профиля подготовки – Безопасность информационных систем и технологий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационная безопасность и защита информации
2.1.2	Программно-аппаратные-средства обеспечения информационной безопасностью
2.1.3	Сети ЭВМ
2.1.4	Безопасность баз данных
2.1.5	Основы информационной безопасности
2.1.6	Программно-аппаратные-средства обеспечения информационной безопасностью
2.1.7	Безопасность баз данных
2.1.8	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность информационных систем
2.2.2	Организационно-правовое обеспечение информационных систем
2.2.3	Безопасность информационных систем
2.2.4	Организационно-правовое обеспечение информационных систем

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
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
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-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 понятия в области информационной безопасности; Современные методы и средства защиты информации в вычислительных системах и сетях; Основные методы аутентификации и авторизации пользователей; Угрозы информационной безопасности и методы их предотвращения; Техники анализа уязвимостей и методы предотвращения атак на информационные системы; Основные методы и средства обнаружения вторжений; Техники инцидентного реагирования и восстановления информации.
3.2	**Уметь:**
3.2.1	Разрабатывать и использовать средства защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах; Оценивать уровень защиты криптографических систем и выбирать подходящие методы в зависимости от контекста использования; Анализировать уязвимости информационных систем и разрабатывать меры по их предотвращению; Совместно работать в группе для решения задач, связанных с обеспечением безопасности информационных систем и технологий.
3.3	**Владеть:**
3.3.1	Навыками анализа уязвимости информационных систем и разработки плана мер по обеспечению их безопасности; Навыками оценки рисков, связанных с использованием информационных систем и технологий, и разработки плана их минимизации; Навыками сравнения, выбора и использования средств защиты информации в зависимости от задач и условий их применения; Навыками анализа и тестирования систем защиты информации с целью определения их эффективности и обеспечения их надежности; методами и средствами защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи, установлении подлинности автора передаваемых сообщений.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Системы аутентификации					
1.1	Виды аутентификации. Протоколы аутентификации в сетях. /Лек/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
1.2	Угрозы и защита от атак на аутентификацию. /Пр/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
1.3	Виды аутентификации. Протоколы аутентификации в сетях. /Ср/	7	5	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.2 Л1.1Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
	Раздел 2. Системы разграничения прав доступа					

2.1	Концепция привилегий в системе.Модели разграничения прав доступа. /Лек/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
2.2	Обход прав доступа. /Пр/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
2.3	Концепция привилегий в системе.Модели разграничения прав доступа.Обход прав доступа. /Ср/	7	5	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
	Раздел 3. Системы обнаружения атак					
3.1	Методы обнаружения атак и вторжений.Технологии мониторинга сетевого трафика. /Лек/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
3.2	Интеграция СОАВ в систему безопасности. /Пр/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
3.3	Методы обнаружения атак и вторжений.Технологии мониторинга сетевого трафика. Интеграция СОАВ в систему безопасности. /Ср/	7	10	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
	Раздел 4. Аудит безопасности					
4.1	Методологии проведения аудита безопасности. Реагирование на инциденты и восстановление. /Лек/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
4.2	Политика безопасности. /Пр/	7	4	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	

4.3	Методологии проведения аудита безопасности. Реагирование на инциденты и восстановление. Политика безопасности. /Ср/	7	5	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
	Раздел 5. Работа над проектом					
5.1	Самостоятельная работа над проектом. /Ср/	7	15	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	
	Раздел 6. Зачет					
6.1	Зачет /Зачёт/	7	0	ПК-5.1 ПК-5.2 ПК-5.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.3 Л1.1 Л1.2Л2.3 Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 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	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018,	1
Л1.2	Зенков А. В.	Информационная безопасность и защита информации: Учебное пособие для вузов	Москва: Юрайт, 2022,	1
Л1.3	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,	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018,	1
Л2.2	Жук А.П., Жук Е.П.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018, http://znanium.com/go.php?id=937469	1
Л2.3	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2018,	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Фомин Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: Учебно-методическое пособие	Саратов: Вузовское образование, 2018,	1
Л3.2	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: НГТУ, 2019,	1
Л3.3	Никулин В. В.	Информационная безопасность. Лабораторный практикум: учебно-методическое пособие для студентов направления подготовки 09.03.03 прикладная информатика	Брянск: Брянский ГАУ, 2021,	1
Л3.4	Фомин Д. В.	Информационная безопасность: Учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения	Саратов: Вузовское образование, 2018,	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. 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,локальная вычислительная сеть с выходом в глобальную сеть Internet.