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
Управление информационной безопасностью
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 **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 64
самостоятельная работа 35
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 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	35	35	35	35
Часы на контроль	45	45	45	45
Итого	144	144	144	144

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

Рабочая программа дисциплины
Управление информационной безопасностью

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.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Безопасность информационных систем
2.1.2	Рзаработка и эксплуатация защишенных информационных систем
2.1.3	Теория информационных процессов и систем
2.1.4	Безопасность информационных систем
2.1.5	Рзаработка и эксплуатация защишенных информационных систем
2.1.6	Теория информационных процессов и систем
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Моделирование систем
2.2.2	Инструментальные средства информационных систем
2.2.3	Информационная безопасность и защита информации
2.2.4	Качество информационных систем
2.2.5	Надежность информационных систем
2.2.6	Программно-аппаратные-средства обеспечения информационной безопасностью
2.2.7	Безопасность баз данных
2.2.8	Информационная безопасность и защита информации
2.2.9	Качество информационных систем
2.2.10	Надежность информационных систем
2.2.11	Программно-аппаратные-средства обеспечения информационной безопасностью
2.2.12	Безопасность баз данных

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-6.1: Демонстрирует знания этапов и методов разработки технической документации на продукцию в сфере информационных технологий и технических документов информационно-методического и маркетингового назначения

ПК-6.2: Разрабатывает техническую документацию на продукцию в сфере информационных технологий и технических документов информационно-методического и маркетингового назначения

ПК-6.3: Управляет технической информацией

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 принципы информационной безопасности. Законы и нормативные акты, регулирующие область информационной безопасности. Основные угрозы информационной безопасности и способы их предотвращения. Принципы управления рисками в области информационной безопасности.
3.2	**Уметь:**
3.2.1	Анализировать уязвимости и риски в информационных системах. Разрабатывать и внедрять политику информационной безопасности в организации. Организовывать проверки и аудит систем информационной безопасности. Планировать и реализовывать меры по защите информации..
3.3	**Владеть:**
3.3.1	Навыками работы с системами защиты информации (антивирусное ПО, файрволы и т.д.). Навыками мониторинга информационных систем. Навыками анализа и управления рисками в области информационной безопасности. Навыками реагирования на инциденты информационной безопасности и восстановления системы после возникновения таких инцидентов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Основы информационной безопасности					
1.1	Основные принципы защиты информации. Законы и нормативные акты в области информационной безопасности. Международные стандарты и методологии в области информационной безопасности. /Лек/	6	8	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

1.2	Определение уязвимостей информационных систем. /Лаб/	6	8	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.3	Основные принципы защиты информации. Законы и нормативные акты в области информационной безопасности. Международные стандарты и методологии в области информационной безопасности. Определение уязвимостей информационных систем. /Ср/	6	5	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 2. Управление рисками в информационной безопасности					
2.1	Управление рисками и разработка политики информационной безопасности. Методы оценки эффективности мер по защите информации. Расследование инцидентов информационной безопасности. Разработка плана восстановления после инцидентов информационной безопасности. /Ср/	6	5	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 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	Управление рисками и разработка политики информационной безопасности. Методы оценки эффективности мер по защите информации. Расследование инцидентов информационной безопасности. /Лек/	6	8	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.3	Разработка плана восстановления после инцидентов информационной безопасности. /Лаб/	6	6	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 3. Технологии и методы защиты информации					
3.1	Криптографические методы защиты информации. Сетевая безопасность и защита от кибератак. Физическая безопасность информационных систем. /Лек/	6	8	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	Управление доступом и идентификация в информационных системах. Практическое применение криптографических методов защиты информации. /Лаб/	6	6	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.3	Управление доступом и идентификация в информационных системах. Практическое применение криптографических методов защиты информации. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

	Раздел 4. Аудит и контроль информационной безопасности					
4.1	Методы и техники аудита систем информационной безопасности. Использование инструментов и систем для контроля информационной безопасности. /Лек/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.2	Мониторинг безопасности информационных систем. /Лаб/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.3	Методы и техники аудита систем информационной безопасности. Использование инструментов и систем для контроля информационной безопасности. Мониторинг безопасности информационных систем. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 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-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
5.2	Планирование и управление проектами безопасности. /Лаб/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 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-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 6. Работа над проектом					
6.1	Самостоятельная работа над проектом. /Лаб/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
6.2	Самостоятельная работа над проектом. /Ср/	6	10	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 7. Экзамен					
7.1	Экзамен /Экзамен/	6	45	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.5 Л1.4 Л1.2 Л1.1 Л1.3Л2.1 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	Баранова Е.К., Бабаш А.В.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИО, 2020,	1
Л1.2	Анисимов А. А.	Менеджмент в сфере информационной безопасности: Учебное пособие	Москва, Саратов: ?нтернет-Университет ?нформационных Технологий (?НТУ?Т), Ай Пи Ар Медиа, 2020,	1
Л1.3	Башлы П. Н., Бабаш А. В., Баранова Е. К.	Информационная безопасность и защита информации: Учебное пособие	Москва: Евразийский открытый институт, 2012,	1
Л1.4	Жукова М. Н.	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012,	1
Л1.5	Золотарев В. В.	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков	Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010,	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Партыка Т. Л., Попов И.И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2021,	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2	Шилов А.К.	Управление информационной безопасностью: Учебное пособие	Ростов-на-Дону: ?здательство Южного федерального университета (ЮФУ), 2018,	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,	1
Л3.2	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2021,	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.