

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2023 11:20:52
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.О.28 Информационная безопасность предприятия***

обязательная часть

Направление

10.03.01
код

Информационная безопасность
наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;	ОПК-1.4.1. Сети и системы передачи информации	Обучающийся должен: знать навыки определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
	ОПК-1.4.2. Информационная безопасность предприятия	Обучающийся должен: уметь принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
	ОПК-1.4.3. Подготовка к процедуре защиты и защита выпускной квалификационной работы	Обучающийся должен: владеть навыками принятия участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Данная дисциплина (модуль) включена в раздел "Б1.Б.5 Дисциплины (модули)" основной профессиональной образовательной программы и относится к базовой (общепрофессиональной) части.

Дисциплина изучается на 5 курсе, в 9 и 10 семестре.

Дисциплина изучается на 5 курсе в 9, 10 семестрах

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 10 зач. ед., 360 акад. ч.

Объем дисциплины	Всего часов
	Очно-заочная обучения
Общая трудоемкость дисциплины	360
Учебных часов на контактную работу с преподавателем:	
лекций	44
практических (семинарских)	50
лабораторных	50
другие формы контактной работы (ФКР)	1,4
Учебных часов на контроль (включая часы подготовки):	34,8
зачет	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	179,8

Формы контроля	Семестры
зачет	9
экзамен	10

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	Угрозы информационной безопасности в информационных системах.	32	38	35	134,9
1.1	Основные понятия информационной безопасности. Угрозы	11	13	10	45

	информационной безопасности в информационных системах.				
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	11	13	15	45
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	10	12	10	45
2	Современные методы и средства анализа и управление рисками информационных систем компаний.	11	12	10	45
2.1	Правовые меры обеспечения информационной безопасности.	11	12	10	45
	Итого	43	50	45	179,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Угрозы информационной безопасности в информационных системах.	
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Вредительские программы.
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Роль стандартов ИБ. Оранжевая книга как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка

		информационных рисков. Обработка информационных рисков. Внедрение процедур системы управления ИБ. Расчет рисков по угрозе информационной безопасности. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность
2	Современные методы и средства анализа и управление рисками информационных систем компаний.	
2.1	Правовые меры обеспечения информационной безопасности.	Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Угрозы информационной безопасности в информационных системах.	
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Вредительские программы.
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Роль стандартов ИБ. Оранжевая книга как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	Внедрение процедур системы управления ИБ. Расчет рисков по угрозе информационной безопасности. Описание архитектуры ИС.

		Расчет рисков по угрозе конфиденциальность
2	Современные методы и средства анализа и управление рисками информационных систем компаний.	
2.1	Правовые меры обеспечения информационной безопасности.	Основные направления обеспечения информационной безопасности

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Угрозы информационной безопасности в информационных системах.	
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Роль стандартов ИБ. Оранжевая книга как оценочный стандарт.Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.Стандарты управления информационной безопасностью
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков.
2	Современные методы и средства анализа и управление рисками информационных систем компаний.	
2.1	Правовые меры обеспечения информационной безопасности.	Основные направления обеспечения информационной безопасности