Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2023 10:52:19
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a198149ad36

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 ***Основы управления информационной безопасностью***

Блок Б1, базовая часть, Б1.Б.36
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01 код — ***Информационная безопасность*** наименование направления

Программа

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

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	1 этап: Знания	Обучающийся должен знать: содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем (АС) и подсистем безопасности АС
	2 этап: Умения	Обучающийся должен уметь: определять комплекс мер для обеспечения информационной безопасности АС
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: профессиональной терминологией в области управления ИБ
Способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	1 этап: Знания	Обучающийся должен знать: методику формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
	2 этап: Умения	Обучающийся должен уметь: пользоваться методикой формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
	3 этап: Владения	Обучающийся должен владеть:

	(навыки / опыт деятельности)	навыками формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	1 этап: Знания	Обучающийся должен знать: сновные методы управления информационной безопасностью
	2 этап: Умения	Обучающийся должен уметь: разрабатывать предложения по совершенствованию системы управления ИБ АС
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках базовой части. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Теория информации», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Цифровая экономика», «Теоретические основы защиты информации», «Сети и системы передачи информации», «Техническая защита информации», «Электронный бизнес».

Дисциплина изучается на 4 курсе в 7 семестре

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 3 зач. ед., 108 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18
лабораторных	18
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	24

Формы контроля	**Семестры**

экзамен	7

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	**Система управления информационной безопасностью**	**12**	**18**	**18**	**24**
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	2	0	0	3
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	2	2	0	3
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	2	2	0	3
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	2	2	0	3
1.5	Правовые меры обеспечения информационной безопасности.	2	2	4	3
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	2	2	4	3
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	0	4	4	3
1.8	Протоколирование и аудит, шифрование, контроль целостности	0	4	6	3
	Итого	**12**	**18**	**18**	**24**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Система управления информационной безопасностью**	
1.1	Основные понятия информационной	Понятие информационной безопасности.

	безопасности. Угрозы информационной безопасности в информационных системах.	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.
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании.Методика FRAP. Методика OCTAVE (октэйв). Методика RiskWatch (риск вэтч).
1.5	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.
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Система управления информационной безопасностью**	
1.5	Правовые меры обеспечения информационной безопасности.	ЛАБОРАТОРНАЯ РАБОТА № 1 ПРАВОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	ЛАБОРАТОРНАЯ РАБОТА №2: РЕАЛИЗАЦИЯ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	ЛАБОРАТОРНАЯ РАБОТА № 3 ПРИМЕНЕНИЕ ИНВЕРСИОННОГО МЕТОДА ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.
1.8	Протоколирование и аудит, шифрование, контроль целостности	ЛАБОРАТОРНАЯ РАБОТА №4: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Система управления информационной безопасностью**	
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Сертификация СУИБ на соответствие ISO 27001.
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	Разработка политики ИБ
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Разработка методики оценки рисков ИБ
1.5	Правовые меры обеспечения информационной безопасности.	Нормативные акты предприятия по информационной безопасности
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Служба безопасности предприятия

1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Проведение внутреннего аудита ИБ
1.8	Протоколирование и аудит, шифрование, контроль целостности	Организация работы службы безопасности предприятия