АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность

Магистерская программа: «Безопасность автоматизированных систем»

Б1.О.07 «Защищенные информационные системы»

№	Индекс	Наименование	Семестр 3											Итого за курс											Каф	Сем
			Контроль	Академических часов								З.е.	Недель	Контроль	Академических часов								З.е.	Недель		
				Всего	Контакт	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Контакт	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
8	Б1.О.07	Защищенные информационные системы	Экз, РГР	180	52	18	16	18		56	36	4		Экз, РГР	180	52	18	16	18		56	36	4		15	3

Формируемые компетенции: ОПК-1, ОПК-2

Содержание дисциплины

№	Наименование видов занятий и тематик, содержание
1	**Лекционные занятия**, количество - 9 по 2 часа. Тема 1. Анализ угроз информационной безопасности 1.1. Проблемы безопасности информационных систем (2 часа). Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Проблемы безопасности IP-сетей. Способы обеспечения информационной безопасности. Пути решения проблемы защиты информации. Тема 2. Политика безопасности. 1.2. Основные понятия политики безопасности. (2 часа). Описание проблемы. Область применения. Позиция организации. Распределение ролей и обязанностей. Управленческие меры обеспечения информационной безопасностью. 1.3. Структура политики безопасности организации (2 часа). Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Тема 3. Архитектура защищенной информационной системы 1.4. Концепция глобального управления безопасностью (2 часа). Концепция GSM (Global Security Management). Основные свойства GSM. Глобальная и локальная политика безопасности. 1.5. Функционирование системы управления средствами безопасности. (2 часа). Назначение основных средств безопасности. Защита ресурсов. Управление средствами защиты. Управление пользователями и правами доступа. Аудит и мониторинг безопасности информационных систем. 1.6. Обеспечение безопасности облачных систем (2 часа). Общие требования к безопасности облачных технологий. Безопасность сете-

№	Наименование видов занятий и тематик, содержание
	вой части облака. Безопасность серверной части облака. Безопасность хранения данных и приложений. 1.7. Средства защиты информационных систем (2 часа). Организация защиты от вирусов. Межсетевые экраны. Средства обнаружения и предотвращения вторжений. Средства предотвращения утечек. Средства шифрования. Средства двухфакторной аутентификации. Однократная аутентификация. Ложные информационные системы. Тема 4. Тестирование защиты 1.8. Модель опасностей (2 часа). Декомпозиция приложения. Ранжирование интерфейсов по степени уязвимости. Атаки по классификации STRIDE. Создание инструментов для поиска дефектов. 1.9. Создание тест-планов на основании модели опасностей (2 часа). Создание тест-плана. Определение «поверхности поражения». Определение основных векторов атаки. Тестирование с шаблонами безопасности. Сквозное тестирование.
2	**Лабораторные работы**, количество - 4 по 4 часа. 2.1. Установка защищенной информационной системы. Цель лабораторной работы: Провести установку программного обеспечения криптошлюза и настройку сетевого взаимодействия между ним и центром управления сетью. 2.2. Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа. Цель лабораторной работы: Демонстрация настроек межсетевого экрана 2.3 Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами. 2.4 Мониторинг состояния компонентов системы и передаваемого трафика, настройка реакции на события.
3	**Практические занятия**, количество – 9 по 2 часа. 3.1. Способы обеспечения информационной безопасности. 3.2. Меры обеспечения информационной безопасностью. 3.3. Процедуры безопасности. 3.4. Глобальная и локальная политика безопасности. 3.5. Управление пользователями и правами доступа. 3.6. Безопасность облачных технологий. 3.7. Средства обнаружения и предотвращения вторжений. 3.8. Средства предотвращения утечек информации. 3.9. Сквозное тестирование.
4	**Расчетно-графическая работа** «Разработка модели защищенной информационные системы». Выполнение индивидуального задания, предполагающего разработку модели защищенной информационной системы, реализацию и проверку ее работы.
5	**Самостоятельная работа** студентов: 5.1. Подготовка к защите лабораторных работ. 5.2. Подготовка к практическим занятиям.

№	Наименование видов занятий и тематик, содержание
	5.2. Самостоятельное изучение теоретических материалов по следующим вопросам. Методы оценки рисков информационной безопасности (ИБ). Процесс оценки рисков ИБ: идентификация рисков, анализ рисков, оценивание рисков, обработка рисков. Процесс управления риском ИБ. Программный инструментарий для управления рисками. Методика CRAMM. Методика ГРИФ. Методика RiskWatch. Методика CORAS. Методика MSAT. 5.3. Выполнение расчетно-графической работы.

Год начала подготовки _____2024_____

Образовательный стандарт ___№ 1455_ от «26» ноября 2020 г. _____