

Направление подготовки 10.04.01 «Информационная безопасность»
 Магистерская программа «Безопасность автоматизированных систем»
 Документ подписан
 ЭЛЕКТРОННОЙ ПОДПИСЬЮ



Владелец: Федулов Александр Сергеевич
 Сертификат: 5A022291D0DE01CCADCB2B81371C7969
 Действителен: 06.05.2025 - 30.07.2026

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность

Магистерская программа: «Безопасность автоматизированных систем»

Б1.О.07 «Защищенные информационные системы»

№	Индекс	Наименование	Контроль	Семестр 3								З.е.		Неделя	Итого за курс								Каф	Сем		
				Всего	Контакт	Лек	Академических часов			КРП	СР	Контроль	Всего		Контакт	Лек	Академических часов			КРП	СР	Контроль			З.е.	Неделя
							Лаб	Пр	КРП								Лаб	Пр	КРП							
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	<p>Лекционные занятия, количество - 9 по 2 часа.</p> <p>Тема 1. Анализ угроз информационной безопасности</p> <p>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.</p> <p>Тема 2. Политика безопасности.</p> <p>1.2. Основные понятия политики безопасности. (2 часа). Описание проблемы. Область применения. Позиция организации. Распределение ролей и обязанностей. Управленческие меры обеспечения информационной безопасностью.</p> <p>1.3. Структура политики безопасности организации (2 часа). Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности.</p> <p>Тема 3. Архитектура защищенной информационной системы</p> <p>1.4. Концепция глобального управления безопасностью (2 часа). Концепция GSM (Global Security Management). Основные свойства GSM. Глобальная и локальная политика безопасности.</p> <p>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.</p> <p>1.6. Обеспечение безопасности облачных систем (2 часа). Общие требования к безопасности облачных технологий. Безопасность сете-</p>

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

№	Наименование видов занятий и тематик, содержание
	<p>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.</p> <p>5.3. Выполнение расчетно-графической работы.</p>

Год начала подготовки _____ 2026 _____

Образовательный стандарт (СУОС) от 20.12.2023