

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2023 11:20:51
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.В.08 Системы обнаружения атак**
часть, формируемая участниками образовательных отношений

Направление
10.03.01 **Информационная безопасность**
код 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)
ПК-3. Способен владеть информацией о направлениях развития компьютеров с традиционной (нетрадиционной) архитектурой, о тенденциях развития функций и архитектур проблемно-ориентированных программных систем и комплексов	ПК-3.1. Знания	Обучающийся должен знать: направления развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности.
	ПК-3.2. Умения	Обучающийся должен уметь: программировать для компьютеров с различной современной архитектурой.
	ПК-3.3. Владение навыками	Обучающийся должен владеть навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования

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

Цели изучения дисциплины:

Цели изучения дисциплины:

Дисциплина реализуется в рамках вариативной части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Информационные технологии», «Технологии и методы программирования». К началу изучения дисциплины студенты должны обладать навыками работы на компьютере, знанием основных методов хранения и переработки информации в устройствах персонального компьютера, иметь представление об устройстве современного информационного пространства.

Освоение дисциплины «Системы обнаружения атак» необходимо для развития культуры мышления, обеспечивающей способности к обобщению, анализу и восприятию информации; для понимания сущности и значения информационных технологий и систем в решении хранения, обработки данных. А также для формирования умений использовать специализированные программные средства в своей учебной и профессиональной деятельности.

Дисциплина изучается на 4 курсе в 7 семестре.

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
	Очно-заочная обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических (семинарских)	16
лабораторных	16
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

Формы контроля	Семестры
зачет	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	

1	Основной	16	16	16	59,8
1.1	Обнаружение компьютерных атак	2	2	2	12
1.2	Технология межсетевого экранирования	2	2	2	12
1.3	Организация виртуальных частных сетей	4	4	4	12
1.4	Технологии защищенной обработки информации	4	4	4	12
1.5	Аудит информационной безопасности в компьютерных сетях	4	4	4	11,8
	Итого	16	16	16	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Основной	
1.1	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
1.2	Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования
1.3	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.
1.4	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTSC. Настройка протокола RDP.
1.5	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-

		<p>телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.</p>
--	--	---

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Основной	
1.1	Обнаружение компьютерных атак	
1.2	Технология межсетевого экранирования	
1.3	Организация виртуальных частных сетей	
1.4	Технологии защищенной обработки информации	
1.5	Аудит информационной безопасности в компьютерных сетях	

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Основной	
1.1	Обнаружение компьютерных атак	Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute
1.2	Технология межсетевого экранирования	Защита сетевого трафика с использованием протокола IPSec в Windows NT 5.0. Организация VPN средствами протокола PPTP
1.3	Организация виртуальных частных сетей	Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET»
1.4	Технологии защищенной обработки информации	
1.5	Аудит информационной безопасности в компьютерных сетях	