

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.В.ДВ.05.02 Системы обнаружения атак***

часть, формируемая участниками образовательных отношений

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
2021 г.

Разработчик (составитель)

Мифтахов Э. Н.

ученая степень, должность, ФИО

Стерлитамак 2022

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	3
2. Цели и место дисциплины (модуля) в структуре образовательной программы	3
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	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	4
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	4
4.2. Содержание дисциплины, структурированное по разделам (темам)	4
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	6
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	6
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)	6
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	7

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-2. Способен использовать инструментальные средства и технологии администрирования средств защиты информации в компьютерных системах и сетях	ПК-2.1. знания	Обучающийся должен знать: требования по защите информации, включая использование математического аппарата для решения прикладных задач
	ПК-2.2. умения	Обучающийся должен уметь: проводить разработку и анализ структурных и функциональных схем защищенных компьютерных систем в сфере профессиональной деятельности.
	ПК-2.3. владение навыками	Обучающийся должен владеть: навыками оценивания оптимальности выбора программно-аппаратных средств защиты информации.

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

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 8 семестре.

Дисциплина изучается на 4 курсе в 8 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)	32
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	8

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	
1.2	Технология межсетевого экранирования	2	4	0	12
1.1	Обнаружение компьютерных атак	2	4	0	12
1.5	Аудит информационной безопасности в компьютерных сетях	4	8	0	11,8
1.3	Организация виртуальных частных сетей	4	8	0	12
1.4	Технологии защищенной обработки информации	4	8	0	12
1	Основной	16	32	0	59,8
	Итого	16	32	0	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1.2	Технология межсетевого	Защита сетевого трафика с использованием протокола

	экранирования	IPSec в Windows NT 5.0. Организация VPN средствами протокола PPTP
1.1	Обнаружение компьютерных атак	Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute
1.5	Аудит информационной безопасности в компьютерных сетях	Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз
1.3	Организация виртуальных частных сетей	Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET»
1.4	Технологии защищенной обработки информации	Применение COA Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании»
1	Основной	

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
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
1.1	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.
1.5	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-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.

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	Основной	

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа студентов, предусмотренная учебным планом, должна соответствовать более глубокому усвоению изучаемого материала, формировать навыки исследовательской работы и ориентировать их на умение применять полученные теоретические знания на практике. В процессе этой деятельности решаются задачи:

- научить студентов работать с учебной литературой;
- формировать у них соответствующие знания, умения и навыки;
- стимулировать профессиональный рост студентов, воспитывать творческую активность и инициативу.

Самостоятельная работа студентов предполагает:

- подготовку к занятиям (изучение лекционного материала и чтение литературы);
- оформление отчета по самостоятельной работе;
- подготовку к зачету.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

- чтение и конспектирование рекомендованной литературы,
- проработку учебного материала (по конспектам лекций, учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения;
- решение задач, предлагаемых студентам на лекциях и лабораторных занятиях,
- подготовку к лабораторным занятиям.

Обязательным является выполнение лабораторных работ, которые оформляются в специально отведённой для этого тетради и систематически сдаются на проверку.

Текущий контроль осуществляется в формах:

- опрос студентов;
- домашние работы;
- самостоятельная работа студентов на лабораторных занятиях.

Итоговый контроль:

- зачет.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный

- университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=438331>
2. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие : [16+] / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=480637>
 3. Шаньгин, В. Ф. Информационная безопасность и защита информации : практическое пособие / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2014. – 702 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=260320>

Дополнительная учебная литература:

1. Программно-аппаратные средства защиты информации : учебное пособие : [16+] / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. – Санкт-Петербург : Интермедия, 2018. – 408 с. : схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=481123>
2. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428820>

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
-------	---