ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.03 БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

Подготовка к разработке системы управления информационной безопасностью автоматизированных систем, администрирование подсистем информационной безопасности автоматизированных систем

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.03 Безопасность вычислительных сетей относится к части, формируемой участниками образовательных отношений учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Безопасность вычислительных сетей» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-2	Основы защиты АИС

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-2	Безопасность информации в банковских системах Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика
ПК-3	Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) Безопасность систем баз данных Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)

ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-2.1 Осуществляет выбор и настройку средств защиты информации в компьютерных системах и сетях	*Знать:* организацию взаимодействия в вычислительных сетях *Уметь:* осуществлять настройку основных параметров безопасности сетевого взаимодействия. *Владеть:* Навыками конфигурирования сетевого и телекоммуникационного оборудования для обеспечения безопасности сетевого взаимодействия.
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* перспективные направления обеспечения информационной безопасности в вычислительных сетях; актуальные подходы к реализации безопасного информационного обмена и надежного функционирования компьютерных сетей; типичные уязвимости и способы реализации основных сетевых атак *Уметь:* применять стандартные средства и технологии обеспечения защиты сетевой топологии и безопасной работы вычислительных сетей; организовывать защищенный информационный обмен в компьютерных вычислительных сетях; реализовывать комплекс защитных мероприятий для обеспечения безопасности функционирования вычислительных сетей; строить политики сетевой безопасности и фильтрации сетевого трафика; *Владеть:* навыками анализа сетевых информационных систем с позиции обеспечения информационной безопасности; методикой планирования и обеспечения защитных мероприятий на компьютерных вычислительных сетях; навыками применения защищенных протоколов сетевого обмена, средств контроля доступа и фильтрации трафика в вычислительных сетях и сетевых информационных системах.

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* основные сервисы безопасности в сетях; современные протоколы и принципы построения безопасных сетей передачи данных. *Уметь:* применять современные методы защиты при решении проблем информационной безопасности в сетях. *Владеть:* знаниями о современных методах защиты при решении проблем информационной безопасности в сетях.

4. Объем дисциплины

Объем дисциплины Б1.В.03 Безопасность вычислительных сетей составляет 4 зачетных(ые) единиц(ы) (ЗЕ), (144 академических часов), распределение объёма дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

Вид учебной работы	Итого КР	Итого СР	Семестр №6	
			КР	СР
Лекции (Л)	36		36	
Лабораторные работы (ЛР)				
Практические занятия (ПЗ)	36		36	
Семинары(С)				
Курсовое проектирование (КП)	2		2	
Самостоятельная работа		66		66
Промежуточная аттестация	4		4	
Наименование вида промежуточной аттестации	x	x	Экзамен	
Всего	78	66	78	66

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		лекции	Лабораторная работа	Практические занятия	семинары	Курсовое проектирование	индивидуальные домашние задания (контрольные работы)	Самостоятельноеизучение вопросов	подготовка к занятиям	Промежуточная аттестация	
Тема 1. Основы вычислительных сетей. Сетевая архитектура.	6	4		6				10	4		ПК-3 ПК-3.1 ПК-3.2
Тема 2. Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности.	6	8		4				8	4		ПК-3 ПК-3.1 ПК-3.2
Тема 3. Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX.	6	8		6				8	6		ПК-3 ПК-3.1 ПК-3.2
Тема 4. Глобальная сеть Интернет.	6	6		6				4	4		ПК-3 ПК-3.1
Тема 5. Безопасности сети Интернет.	6	6		6				4	4		ПК-3 ПК-3.1
Тема 6. Комплексная защита подключения к Интернет.	6	4		8				4	6		ПК-3 ПК-3.1 ПК-3.2
Контактная работа	6	36		36		2				4	
Самостоятельная работа	6							38	28		
Объем дисциплины в семестре	6	36		36				38	28	4	x
Всего по дисциплине		36		36		2		38	28	4	

5.2. Темы курсовых работ (проектов)3

1. Анализ системы безопасности вычислительных сетей класса Windows, стратегий ее использования.

2. Анализ системы безопасности вычислительных сетей клона Unix и стратегий ее использования.

3. Для систем клона Unix предполагается решение следующих практических задач: настройка защищенной конфигурации web-портала с использованием средств разграничения прав доступа;

4. Редактирование регистрационных записей и настройка пользователей;

5. Разработка программы определяющей сетевое имя и ip-адрес компьютера (рабочей станции).

6. Настройка комплексной защиты сервера с использованием расширенных атрибутов;

7. Организация разделения дискового пространства между пользователями с использованием механизма квот;

8. Настройка ограничения ресурсов, используемых в процессе работы, для заданной группы пользователей;

9. Настройка межсетевого экрана с заданными требованиями к безопасности;

10. Безопасная настройка сервиса SSH с учетом уязвимостей в версии SSH 1.0.

5.3. Темы индивидуальных домашних заданий (контрольных работ)

не предусмотрены

5.4 Вопросы для самостоятельного изученияпо очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Основы вычислительных сетей. Сетевая архитектура.	Разделение кода и данных между процессами. Экспорт и импорт функций.	10
2	Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности.	Угрозы безопасности ВС. Классификация угроз безопасности ВС. Наиболее распространенные угрозы.	8
3	Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX.	Требования к защите ВС. Понятие защищенной ВС. Подходы к организации защиты.	8
4	Глобальная сеть Интернет.	Анализ атаки «Переполнение буфера системного приложения» и способов защиты от неё.	4
5	Безопасности сети Интернет.	Взлом паролей и защита от взлома.	4

6	Комплексная защита подключения к Интернет.	Взлом паролей UNIX и защита от взлома.	4
		Всего	38

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

Безопасность сетей: учебное пособие. — 2-е изд. — Москва : ИНТУИТ, 2016. — 571 с.

Федорова, В.А. Проектирование физического и канального уровней безопасной вычислительной сети предприятия : учебное пособие / В. А. Федорова. — Москва : МГТУ им. Н.Э. Баумана, 2017. — 20 с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

Дыхан, Л. Б. Безопасность труда при работе на персональной электронно-вычислительной машине (ПЭВМ) : учебное пособие / Л. Б. Дыхан. — Ростов-на-Дону : ЮФУ, 2016. — 128 с.

6.3 Методические материалы для обучающихся по освоению дисциплины

тематический план дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант + .

.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Старший преподаватель, _____ Антонова О.В.

Рабочая программа рассмотрена и одобрена на заседании кафедры Цифровых систем обработки информации и управления, протокол №7 от 22.02.2019

Зав. кафедрой _____ М.Ю.Шрейдер

Программа рассмотрена и утверждена на заседании учебно- методической комиссии Институт управления рисками и комплексной безопасностью, протокол №7 от 23.02.2019 г.

Директор Институт управления рисками
и комплексной безопасностью _____ Яковлева Е.В

.

Дополнения и изменения

в рабочей программе дисциплины Б1.В.03 Безопасность вычислительных сетей на 2022-2023 учебный год.

В программу вносятся следующие изменения:

без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Цифровых систем обработки информации и управления, протокол № 7 от 22.02.2022 г.

Зав. кафедрой М.Ю.Шрейдер