ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.05 БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

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, администрированию.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.05 Безопасность операционных систем относится к части, формируемой участниками образовательных отношений учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Безопасность операционных систем» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-3	Безопасность вычислительных сетей КОИБАС Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) 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-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* основные положения сбора информации и проведения анализа при организации защиты операционных систем *Уметь:* анализировать сложившуюся ситуацию при организации защиты операционных систем *Владеть:* способами и методами анализа защищенности операционных систем

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:* Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. *Уметь:* Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. *Владеть:* Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.

4. Объем дисциплины

Объем дисциплины Б1.В.05 Безопасность операционных систем составляет 3 зачетных(ые) единиц(ы) (ЗЕ), (108 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 №5	
			КР	СР
Лекции (Л)	18		18	

Лабораторные работы (ЛР)				
Практические занятия (ПЗ)	34		34	
Семинары(С)				
Курсовое проектирование (КП)	2		2	
Самостоятельная работа		54		54
Промежуточная аттестация				
Наименование вида промежуточной аттестации	х	х	Экзамен	
Всего	54	54	54	54

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. Защита информации в операционных системах, вычислительных сетях и базах данных.	5	4		4				8	6		ПК-3 ПК-3.1 ПК-3.2
Тема 2. Разграничение доступа.	5	4		4				4	6		ПК-3 ПК-3.1 ПК-3.2
Тема 3. Аутентификация.	5	4		8				4	6		ПК-3 ПК-3.1 ПК-3.2
Тема 4. Аудит.	5	2		8					6		ПК-3 ПК-3.1 ПК-3.2
Тема 5. Защита программ и данных от несанкционированного копирования.	5	2		2					6		ПК-3 ПК-3.1 ПК-3.2

Тема 6. Защита от вредоносных воздействий компьютерных вирусов и программных закладок.	5	2		8					8		ПК-3 ПК-3.1 ПК-3.2
Контактная работа	5	18		34		2					ПК-3, ПК-3.1 ПК-3.2х
Самостоятельная работа	5							16	38		ПК-3 ПК-3.1 ПК-3.2х
Объем дисциплины в семестре	5	18		34				16	38		ПК-3 ПК-3.1 ПК-3.2х
Всего по дисциплине		18		34		2		16	38		

5.2. Темы курсовых работ (проектов)

1. Анализ системы безопасности операционных систем класса Windows стратегий ее использования.

2. Анализ системы безопасности операционных систем 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 изучения по очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Защита информации в операционных системах, вычислительных сетях и базах данных.	Особенности операционных систем. Брандмауэр и другие защитные программы.	8
2	Разграничение доступа.	ОС Windows и Linux	4
3	Аутентификация.	Интерактивные ресурсы	4
		Всего	16

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

Нестеров С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 2-е изд. — Москва : ИНТУИТ, 2016. — 250 с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

Староверова Н. А. Операционные системы : учебник / Н. А. Староверова. — СПб.: Лань, 2019. — 308 с.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисицплины

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.05 Безопасность операционных систем 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