Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.3.1 Защита информации в высокопроизводительных системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.В.Э.3.1 Защита информации в высокопроизводительных системах*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "9" марта 2023 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — Н.П. Мошуров
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации 156331

© Мошуров Н.П., 2023
© ОГУ, 2023

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Изучение теоретических основ и получение практических навыков защиты безопасных высокопроизводительных систем.

Задачи:

- изучение операционной системы Astra Linux Special Edition на базе ядра Linux;
- изучение методов искусственного интеллекта для защиты информации в высокопроизводительных и облачных системах;
- изучение основ работы с системами управления контейнерами, их применения для защиты облачных систем;
- изучение основ работы с системами управления облачными ресурсами.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-3 Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	ПК*-3-В-1 Знает основные требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей ПК*-3-В-2 Способен осуществлять разработку и тестирование средств защиты информации компьютерных систем и сетей ПК*-3-В-3 Владеет основными методами защиты информации компьютерных систем и сетей	**Знать:** - принципы функционирования программно-аппаратных средств защиты информации; - основные методы искусственного интеллекта; - основные классификации информационных систем по степени защищенности, методы оценки защищенности компьютерных систем по различным критериям, основные угрозы информационной безопасности. **Уметь:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		- использовать современные среды разработки для отладки и тестирования программного обеспечения; - производить установку современных программно-аппаратных средств; - обеспечения информационной безопасности для высокопроизводительных систем; - конфигурировать программно-аппаратные средства защиты информации, включая защищенные операционные системы, систему управления заданиями, системы управления базами данных в высокопроизводительных системах. **Владеть:** - навыками наладки, тестирования и установки современных программно-аппаратных средств; - обеспечения информационной безопасности для высокопроизводительных систем; - навыками написания кода, исправления ошибок компиляции в современных средах разработки программного обеспечения; - навыками практического использования современных инфраструктур на базе высокопроизводительных и облачных систем.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**74,25**	**74,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	44	44
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**69,75** *15* *34* *20,75*	**69,75** *15* *34* *20,75*
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение	6	2			4
2.	Операционная система Astra Linux Special Edition на базе ядра Linux, для комплексной защиты информации и построения защищённых автоматизированных систем	38	8		12	18
3.	Методы искусственного интеллекта для защиты информации	30	6		10	14
4.	Системы управления контейнерами	38	8		12	18
5.	Системы управления облачными ресурсами	32	6		10	16
	Итого:	144	30		44	70
	Всего:	144	30		44	70

4.2 Содержание разделов дисциплины

1 Введение. Распределенные вычислительные системы, высокопроизводительные и облачны системы. Архитектуры и принципы функционирования систем. Модели облачных сервисов. Общие принципы защиты информации в высокопроизводительных и облачных системах.

2 Операционная система Astra Linux Special Edition на базе ядра Linux.

Классификация ОС по режиму обработки задач, по вариантам реализации многозадачности, по критериям эффективности, по способу взаимодействия с компьютером, по организации работы с вычислительной системой, по наличию средств поддержки многопроцессорной обработки, по организации работы с вычислительной сетью.

Обзор архитектуры ОС семейства Unix, история возникновения и эволюция, архитектура системы и ядра, общие особенности систем семейства Unix; обзор особенностей современных систем Unix (Linux).

Критерии эффективности мультипрограммных систем; системы пакетной обработки; системы разделения времени; системы реального времени; симметричная и ассиметричная мультипроцессорная обработка.

Каналы связи (конвейеры), именованные каналы, очереди сообщений, разделяемая память.

Цели и задачи файловой системы, типы файлов, атрибуты файла, доступ к файлам, операции над файлами, иерархическая структура каталогов, операции над директориями, физическая организация жесткого диска, особенности загрузки ОС, монтирование.

Обеспечение безопасности: конфиденциальность, целостность и доступность данных, типы угроз, политика безопасности. Атаки на систему безопасности: отказ в обслуживании, повышение уровня полномочий, несанкционированный доступ, вирусы, троянские программы. Базовые технологии безопасности: ограничение сетевого доступа, шифрование, аутентификация, авторизация, аудит, ресурсные квоты.

3 Методы искусственного интеллекта для защиты информации. Нейронные сети.

Принципы работы, алгоритмы обучения. Виды нейронных сетей. Типы задач, решаемых с помощью нейронных сетей. Области применения нейронных сетей в информационной безопасности. Применение нейронной сети для реализации системы обнаружения вторжений (IDS). Работа с нейронными сетями в Matlab на примере решения задач по защите информации в высокопроизводительных и облачных системах.

Нечеткие множества, функции принадлежности. Виды функций принадлежности. Операции над нечеткими множествами. Нечеткие отношения. Комбинация нечетких отношений. Логическая переменная. Нечеткий логический вывод и его сравнение с классическим modus ponens. Правило Мамдани. Разработка системы нечеткого логического вывода с использованием Matlab на примере задачи информационной безопасности.

Понятия эволюционных оптимизационных методов: особь, популяция, хромосома, генетические операторы (селекция, скрещивание, мутация), целевая функция оценки приспособленности, генетический алгоритм. Структура генетического алгоритма. Способы представления хромосом. Различные варианты реализации генетических операторов в зависимости от способа представления хромосом. Критерии остановки работы генетического алгоритма. Понятие генетического алгоритма. Типовые задачи, решаемые с помощью генетического алгоритма. Решение задач информационной безопасности, включая задачи защиты высокопроизводительных и облачных систем, с использованием генетического алгоритма в Matlab.

3 Системы управления контейнерами. Основные понятия Docker: образы, контейнеры,репозитарии, тома. Типовые команды Docker для работы с образами, контейнерами и репозитариями и томами. Связывание контейнеров в Docker. Устройство сети между контейнерами в Docker. Команды для работы с сетью. Инструменты, расширяющие возможности Docker - Compose. Machine, Swarm, Registry, Kubernetes. Основные понятия Proxmox. Сравнениес Docker. Базовые операции для работы с контейнерами и виртуальными машинами. Использования Dockeri Proxmox для разработки защищенных микросервисных приложений.

4 Системы управления облачными ресурсами. Система OpenNebula. Архитектура, основные компоненты. Основные команды для работы с образами и виртуальными машинами. Использование OpenNebula для разработки защищенных облачных приложений.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	2	Установление типа файловой системы, использование системных вызовов для доступа к параметрам таблицы разделов из основной загрузочной записи на жестком диске.	6
2.	2	Моделирование функций файловой системы. С использованием жестких и символических ссылок.	6
3.	3	Использование нейронных сетей для решения задач	6

		информационной безопасности	
4.	3	Использование нечеткой логики для решения задач информационной безопасности	4
5.	4	Решение оптимизационных задач в информационной безопасности с помощью генетического алгоритма	6
6.	4	Основы использования системы управления контейнерами Docker. Создание образов с использованием Dockerfile	6
7.	5	Работа с облачной системой OpenNebula	6
8.	5	Работа с облачной системой Microsoft Azure	4
		Итого:	44

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст] : учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. : ил. - Библиогр.: с. 524-529. - Предм. указ.: с. 530-542. - ISBN 5-94074-383-8.

2. Попок, Л. Е. Технологии облачных вычислений : учебное пособие / Л. Е. Попок, Д. А. Замотайлова, Д. Н. Савинская. — Краснодар : КубГАУ, 2019. — 66 с. — ISBN 978-5-00097-873-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254231

5.2 Дополнительная литература

1. Шматов, Г. П. Нейронные сети и генетический алгоритм : учебное пособие / Г. П. Шматов. — Тверь : ТвГТУ, 2019. — 200 с. — ISBN 978-5-7995-1007-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171312

2. Парфенов, Д. В. Параллельные и распределенные вычисления : учебное пособие / Д. В. Парфенов, Д. А. Петрусевич. — Москва : РТУ МИРЭА, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265658

5.3 Периодические издания

1. Информация и безопасность : журнал. - М. : Агентство "Роспечать".
2. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".
3. Системы безопасности : журнал. - М.: Агентство "Роспечать".

5.4 Интернет-ресурсы

1. Нейронные сети для начинающих. Часть 1. – Режим доступа: https://habrahabr.ru/post/312450/

2. Нейронные сети для начинающих. Часть 2. – Режим доступа: https://habrahabr.ru/post/313216/

3. Управление облаком на open-source софте. – Режим доступа: https://habrahabr.ru/company/depocomputers/blog/145826/

4. https://www.intuit.ru/studies/courses/102/102/info – «Интуит. Национальный открытый университет». Курсы, МООК: Безопасность сетей.

5. https://www.intuit.ru/studies/courses/1013/172/info– «Интуит. Национальный открытый университет». Курсы, МООК: Введение в защиту информации от внутренних ИТ-угроз.

6. https://www.intuit.ru/studies/courses/3528/770/info– «Интуит. Национальный открытый университет». Курсы, МООК: Облачные технологии управления малым и средним бизнесом.

7. https://www.intuit.ru/studies/courses/607/463/info– «Интуит. Национальный открытый университет». Курсы, МООК: Введение в нейронные сети.

8. https://intuit.ru/studies/courses/91/91/info– «Интуит. Национальный открытый университет». Курсы, МООК: Основы работы в ОС Linux

9. https://intuit.ru/studies/courses/37/37/info– «Интуит. Национальный открытый университет». Курсы, МООК: Операционная система Linux

10. Комплексное обеспечение информационной безопасности автоматизированных систем : учебное пособие / составители М. А. Лапина [и др.]. — Ставрополь : СКФУ, 2016. — 242 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155111

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО
4. Система управления контейнерами Docker текущей версии. Доступна бесплатно в рамках лицензии Apache 2.0. Разработчик: компания Docker Inc. Режим доступа: https://www.docker.com/

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерным и мультимедийным оборудованием. Рабочие станции студентов и преподавателя объединены в локальную сеть с подключением к Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным проектором и экраном.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки с процессором IntelCore 2 Duo;
- мониторы модели Samsung 793 DF.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.