Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.В.ОД.5 Защита информации в высокопроизводительных системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

Разработка защищенного программного обеспечения
(наименование направленности (профиля) образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 3 от "14" декабря 2017 г.

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

Исполнители:
Доцент *подпись* 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 комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

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

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:
Изучение теоретических основ и получение практических навыков защиты безопасных высокопроизводительных систем.

Задачи:
- 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 обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.22 Языки программирования, С.1.Б.23 Методы программирования, С.1.Б.28 Основы информационной безопасности, С.1.Б.41.7 Параллельное программирование*

Постреквизиты дисциплины: *С.2.Б.П.3 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: - основные принципы работы высокопроизводительных и облачных систем, необходимые для работы специалиста в области компьютерной безопасности. **Уметь:** - использовать инструменты командной строки, необходимые для выполнения команд в высокопроизводительных и облачных системах. **Владеть:** - навыками развертывания, настройки и адаптации высокопроизводительных и облачных систем.	ОК-5 способностью понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать: - основные тенденции в развитии высокопроизводительных вычислений и облачных систем. **Уметь:** -использовать встроенные и внешние средства защиты высокопроизводительных и облачных систем. **Владеть:** - навыками практического использования современных инфраструктур на базе высокопроизводительных и облачных систем.	ОПК-7 способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
	общего и специального назначения
Знать: - основные классификации информационных систем по степени защищенности, методы оценки защищенности компьютерных систем по различным критериям, основные угрозы информационной безопасности. **Уметь:** - определять основные этапы теоретических и научно-исследовательских работ по оценке защищенности распределенных, облачных и высокопроизводительных систем. **Владеть:** - навыками проведения экспериментально-исследовательских работ по сертификации средств защиты для распределенных, облачных и высокопроизводительных систем.	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
Знать: - принципы функционирования программно-аппаратных средств защиты информации. **Уметь:** - конфигурировать программно-аппаратные средства защиты информации, включая защищенные операционные системы, систему управления заданиями, системы управления базами данных в высокопроизводительных системах. **Владеть:** - навыками практического использования современных инфраструктур на базе высокопроизводительных и облачных систем.	ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
Знать: - принципы функционирования современных программно-аппаратных средств обеспечения информационной безопасности для высокопроизводительных систем. **Уметь:** - производить установку современных программно-аппаратных средств обеспечения информационной безопасности для высокопроизводительных систем. **Владеть:** - навыками наладки, тестирования и установки современных программно-аппаратных средств обеспечения информационной безопасности для высокопроизводительных систем.	ПК-18 способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
Знать: - основные методы искусственного интеллекта. **Уметь:** - применять методы искусственного интеллекта для оценки защищенности разрабатываемого программного обеспечения для высокопроизводительных и облачных систем. **Владеть:** - навыками использования математического пакета Matlab для применения методов искусственного интеллекта.	ПСК-1 способностью использовать современные технологии программирования для разработки защищенного программного обеспечения
Знать:	ПСК-2 способностью к

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- виды современных инструментов для разработки и тестирования программного обеспечения. **Уметь:** использовать современные среды разработки для отладки и тестирования программного обеспечения. **Владеть:** – навыками написания кода, исправления ошибок компиляции в современных средах разработки программного обеспечения.	освоению современных сред разработки программного обеспечения и новых образцов программных средств защиты в распределенных компьютерных системах
Знать: - основные типы уязвимостей и недокументированных возможностей. **Уметь:** - пользоваться инструментами анализа исходного кода. **Владеть:** - навыками анализа исходного кода программного обеспечения высокопроизводительных и облачных систем с целью поиска потенциальных уязвимостей и недокументированных возможностей.	ПСК-4 способностью проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**50,25**	**50,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самостоятельное изучение разделов (системы управления облачными ресурсами);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**57,75** 7,75 25 15 5 5	**57,75** 7,75 25 15 5 5
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов		
		всего	аудиторная работа	внеауд. работа

			Л	ПЗ	ЛР	
1.	Введение	6	4			2
2.	Методы искусственного интеллекта для защиты информации	40	10		8	22
3.	Системы управления контейнерами	32	10		4	18
4.	Системы управления облачными ресурсами	30	10		4	16
	Итого:	108	34		16	58
	Всего:	108	34		16	58

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 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. Основныепонятия Proxmox. Сравнениес Docker. Базовые операции для работы с контейнерами и виртуальными машинами. Использования Dockeri Proxmoxдля 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	Использование нейронных сетей для решения задач информационной безопасности	4
2.	2	Использование нечеткой логики для решения задач информационной безопасности	2
3.	2	Решение оптимизационных задач в информационной безопасности с помощью генетического алгоритма	2

4.	3	Основы использования системы управления контейнерами Docker. Создание образов с использованием Dockerfile	4
5.	4	Работа с облачными системами	4
		Итого:	16

5. Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Смоленцев Н. К. MATLAB: Программирование на VisualC#, BorlandC#, JBuilder, VBA [Электронный ресурс] / Смоленцев Н. К. - ДМК Пресс, б. г.. – Режим доступа: http://www.biblioclub.ru/book/86284/

2. 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.

3. Сафонов В. О. Платформа облачных вычислений Microsoft Windows Azure: курс [Электронный ресурс] / Сафонов В. О. - Интернет-Университет Информационных Технологий, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=234656.

5.2 Дополнительная литература

1. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы = Siecineuronowe, algorytm ygenetyczneisystemyrozmyte [Текст] : пер. спол. / Д. Рутковская, М. Пилиньский, Л. Рутковский. - М. : Горячая линия-Телеком, 2007. - 383 с. : ил. - Парал. тит. л. пол. - Библиогр.: с. 379-380. - Предм. указ.: с. 381-383. - ISBN 5-93517-103-1. - ISBN 83-01-12304-4.

2. Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие [Электронный ресурс] / Сергеева Ю. С. - А-Приор, 2011. –Режим доступа: http://www.biblioclub.ru/index.php?page=book&id=72670

3. Джонс М. Т. Программирование искусственного интеллекта в приложениях [Электронный ресурс] / Джонс М. Т. - ДМК Пресс, 2011. –Режим доступа: http://www.biblioclub.ru/index.php?page=book&id=131005

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.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Microsoft Windows текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cf-e05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8

2. Офисный пакет Microsoft Office (Word, Excel, Power Point) текущей версии. Доступен в рамках лицензионного соглашения OVS-ES. Разработчик: компания Microsoft. Режим доступа: https://products.office.com/en/home

3. Система управления контейнерами Dockerтекущей версии. Доступна бесплатно в рамках лицензии Apache 2.0. Разработчик: компания Docker Inc. Режим доступа: https://www.docker.com/

4. Система управления облачными ресурсами OpenNebula текущей версии. Доступна бесплатно в рамках лицензии Apache. Разработчик: OpenNebula Project. Режим доступа: https://opennebula.org/about/faq/

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.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.

Методические указания для обучающихся по освоению дисциплины (модуля) могут быть представлены в виде изданных печатным и (или) электронным способом методических разработок со ссылкой на адрес электронного ресурса, а при отсутствии таковых, в виде рекомендаций обучающимся по изучению разделов и тем дисциплины (модуля) с постраничным указанием глав, разделов, параграфов, задач, заданий, тестов и т.п. из рекомендованного списка литературы.