

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Емельянов Сергей Геннадьевич

Должность: ректор

Дата подписания: 31.12.2020 13:36:24

Уникальный программный ключ:

9ba7d3e34c012eba476ffd2d064cf2781953be730df2374d16f3c0ce536f0fc6

Аннотация дисциплины

Нейросетевые технологии в защите информации

специальность 05.13.19 Методы и системы защиты информации, информационная безопасность

Общая трудоемкость изучения дисциплины составляет 3 ЗЕД (108 часов).

Форма обучения: очная и заочная.

Рабочая программа дисциплины «Нейросетевые технологии в защите информации» составлена на основании федеральных государственных требований к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура), утвержденных приказом Минобрнауки РФ от 16.03.2011 г. № 1365; паспорта специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность», учебного плана ЮЗГУ, программы-минимума кандидатского экзамена, утвержденного приказом Минобрнауки РФ от 08.10.2007 г. № 274.

Цель изучения дисциплины - ознакомление аспирантов с нейросетевым подходом в моделировании различных процессов, принципами их функционирования, методами обучения, использованием в шифровании и распределении ключей, а также в других областях по защите информации.

Задачи дисциплины:

- развитие представлений о математике как об особом способе познания мира, об общности ее понятий и методов;
- способствовать развитию навыков обучения нейронных сетей и нейросетевого моделирования;
- научить основным методам исследования и решения задач защиты информации с помощью нейронных сетей;
- выработать умение самостоятельно расширять знания и проводить анализ прикладных задач информационной безопасности.

В результате изучения дисциплины аспирант должен:

знать:

- методологию исследовательской деятельности, основные проблемы в области информационной безопасности;
- основы культуры научного исследования в информационной безопасности,
- основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач

уметь:

- определять программу проведения исследований,
- использовать и применять их в современных информационно-коммуникационных технологиях
- использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности

владеть:

- планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач
- способностью к критическому анализу результатов научного творчества

-организационными формами и методами проведения научных исследований;
Виды учебной работы: лекции, практические занятия, самостоятельная работа аспирантов.

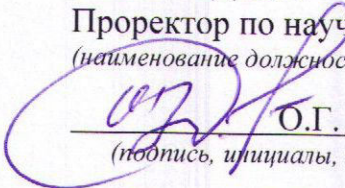
Изучение дисциплины заканчивается кандидатским экзаменом.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Проректор по научной работе
(наименование должности полностью)


О.Г. Добросердов
(подпись, инициалы, фамилия)

« 28 » 06 20 16 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Нейросетевые технологии в защите информации
(наименование дисциплины)

направление подготовки 10.06.01

шифр согласно ФГОС ВО

Информационная безопасность

наименование направления подготовки

Методы и системы защиты информации, информационная безопасность

наименование профиля (специализация подготовки)

квалификация (степень) выпускника: Исследователь. Преподаватель-исследователь

форма обучения очная

(очная, заочная)

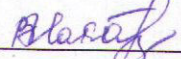
Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (уровень подготовки кадров высшего образования) направления подготовки 10.06.01 «Информационная безопасность», на основании учебного плана профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «27» 06 2016 г.

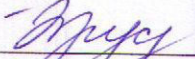
Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 10.06.01 «Информационная безопасность», профиля (специализации) «Методы и системы защиты информации, информационная безопасность» на заседании кафедры информационной безопасности, протокол № 1 от «30» 08 2016 г.

Зав. кафедрой _____  М.О. Таныгин

Разработчик программы _____  Ю.А. Халин

Согласовано:

Директор научной библиотеки _____  В.Г. Макаровская

Начальник отдела аспирантуры и докторантуры _____  О.Ю. Прусова

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 1 «28» 08 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ 

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № « » _____ 20 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № « » _____ 20 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП

1.1 Цель преподавания дисциплины

Курс «Нейросетевые технологии в защите информации» (Б 1.В.ДВ.2.1) входит в вариативную часть общенаучного блока подготовки аспирантов. Он вводит аспирантов в современную проблематику исследований по информационной безопасности. Целью изучения дисциплины является ознакомление аспирантов с нейросетевым подходом в моделировании различных процессов, принципами их функционирования, методами обучения, использованием в шифровании и распределении ключей, а так же в других областях по защите информации.

1.2 Задачи изучения дисциплины

Дисциплина «Нейросетевые технологии в защите информации» предназначена для подготовки аспирантов по направлению 10.06.01 - «Информационная безопасность». Дисциплина играет важную роль в освещении и понимании вопросов информационной безопасности и процессов защиты информации.

Задачами освоения дисциплины являются:

- развитие представлений о математике как об особом способе познания мира, об общности ее понятий и методов;
- способствовать развитию навыков обучения нейронных сетей и нейросетевого моделирования;
- научить основным методам исследования и решения задач защиты информации с помощью нейронных сетей;
- выработать умение самостоятельно расширять знания и проводить анализ прикладных задач информационной безопасности.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие **компетенции**:

ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;

ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

ПК-2 - способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки;

ПК-5 – способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа;

УК-3 – готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач;

УК-6 – способность планировать и решать задачи собственного профессионального и личностного развития.

2 Место дисциплины в структуре образовательной программы

«Нейросетевые технологии в защите информации» представляет дисциплину с индексом Б1.В.ДВ.2.1 вариативной части модуля базовых дисциплин учебного плана направления подготовки 10.06.01 – «Информационная безопасность». Дисциплина «Нейросетевые технологии в защите информации» изучается в 6 семестре аспирантуры, непосредственно связана с дисциплинами специального, естественнонаучного и математического цикла бакалавриата и магистратуры, опирается на освоенные при изучении данных дисциплин знания и умения. Знания, умения и навыки, приобретенные при изучении этой дисциплины, могут использоваться на практиках и при подготовке выпускной квалификационной работы.

3 Содержание и объем дисциплины

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 часов

Таблица 3.1 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
в том числе:	36,1
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	72
Контроль/экс (подготовка к экзамену)	не

Таблица 3.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел, темы дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)	Компетенции
		лек., час	лаб., час	пр., час			
1	2	3	4	5	6	7	8
1	Искусственные нейронные сети. Их классификация.	1, 2 часа	0	1, 2 часа	У-1, У-2, У-4	С 1-2 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
2	Многослойные нейронные сети. Структура. Обоснование возможности применения.	2, 4 часа	0	2, 4 часа	У-1, У-2, У-3, У-6	С 3-6 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
3	Алгоритмы обучения многослойных нейронных сетей.	3, 4 часа	0	3, 4 часа	У-1, У-2, У-3, У-6, МУ-1, МУ-2	КО 7-10 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
4	Самоорганизующиеся нейронные сети.	4, 2 часа	0	4, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 11-12 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
5	Шифрование с использованием нейронных сетей.	5, 2 часа	0	5, 2 часа	У-2, У-3, У-5, У-7, МУ-4	КО 13-14 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
6	Нейросетевой подход к выявлению атак на информационную систему.	6, 4 часа	0	6, 4 часа	У-1, У-2, У-3, У-6, МУ-3, МУ-4	К 15-18 недели	ОПК-2, ОПК-3, ПК-2, ПК-5, УК-3, УК-6
7	ИТОГО	18		18		3	

Э – экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Искусственные нейронные сети. Их классификация.	Мозг человека. Механизмы обучения нейронных систем. Правило обучения Хебба. Принципы ассоциативного обучения. Из истории развития искусственных нейронных сетей. Различные подходы к классификации искусственных нейронных сетей. Искусственный нейрон и принципы его функционирования. Виды функций активации искусственного нейрона.
2	Многослойные нейронные сети. Структура. Обоснование возможности применения.	Многослойные нейронные сети. Теорема Колмогорова и возможности реализации непрерывных функций нейронными сетями. Обоснование алгоритма обучения нейронных сетей обратным распространением ошибок.
3	Алгоритмы обучения многослойных нейронных сетей.	Обобщенное дельта-правило обучения нейронных сетей. Описание алгоритма обучения нейросетей обратным распространением ошибок. Недостатки алгоритма обучения нейросетей обратным распространением ошибок. Выбор адаптивного шага обучения в алгоритме обратного распространения ошибок. Прогнозирование временных рядов многослойными нейронными сетями. Использование логарифмической функции активации в нейронных сетях. Рекуррентные нейронные сети. Описание алгоритма обучения рекуррентной нейронной сети.
4	Самоорганизующиеся нейронные сети.	Самоорганизующиеся нейронные сети, сети Кохоннена. Конкурентное обучение нейронных сетей. Работа нейронной сети по принципу конкуренции. Векторный квантователь. Контролируемое конкурентное обучение нейронных сетей.
5	Шифрование с использованием нейронных сетей.	Нейронные сети как способ шифрования информации. Структура сети с нейросетевым шифратором. Стойкость системы шифрования на основе нейронных сетей.
6	Нейросетевой подход к выявлению атак на информационную систему.	Угрозы, риски и атаки на информационные системы. Нейросетевые технологии распознавания атак на информационные системы. Степень надежности нейросетевого распознавания атак на информационную систему.

3.2 Лабораторные работы и (или) практические занятия

3.2.2 Практические занятия

Таблица 3.5 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Обучение однослойных нейронных сетей с пороговой функцией активации.	2
2	Матричные методы обучения однослойных нейронных сетей.	4
3	Алгоритм обратного распространения ошибки обучений нейронных сетей.	4
4	Векторный алгоритм обучения многослойных нейронных сетей с несколькими выходами.	2
5	Шифрование с использованием нейронных сетей.	2
6	Описание алгоритма обучения нейронной сетевой для выявления атак на информационную систему.	4
Итого		18

3.3 Самостоятельная работа аспирантов (СРС)

Таблица 3.6 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Однослойные нейронные сети с пороговой функцией активации. Линейные нейронные сети. Подготовка <i>доклада</i> и выступление с ним на практическом занятии	2 - 3 неделя	5
2	Многослойные нейронные сети и методы их обучения. Подготовка <i>доклада</i> и выступление с ним на практическом занятии	4 - 5 неделя	5
3	Самоорганизующиеся нейронные сети. Конкретные примеры применения. Подготовка <i>доклада</i> и выступление с ним на практическом занятии	6 - 7 неделя	5
4	Шифрование информации с помощью нейронных сетей. Подготовка <i>доклада</i> и выступление с ним на практическом занятии	8 - 10 неделя	25
5	Написание <i>материалов для выступления на научно-технической конференции с публикацией материалов в сборниках, включенных в РИНЦ.</i>	11-16 неделя	17
6	Развитие международного законодательства в области защиты информации и информационной безопасности Подготовка реферата в рамках предложенной тематики	17 - 18 неделя	15

	Темы реферата – см. Приложение А.		
Итого			72

Общие рекомендации аспирантам изложены в Методических указаниях к выполнению самостоятельной работы.

4 Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки:

- методических рекомендаций, пособий по организации самостоятельной

- работы студентов;

- тем рефератов;

- вопросов к зачету;

- методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

В соответствии с требованиями Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.06.01 – «Информационная безопасность», утвержденного Министерством образования и науки Российской Федерации приказом № 301 от 05.04.2017г.,

реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков аспирантов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами по информационным системам.

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	Семинар на тему «Искусственные нейронные сети. Их классификация»	Компьютерная презентация	2
2	Семинар на тему «Многослойные нейронные сети. Структура. Обоснование возможности применения»	Разбор конкретных ситуаций	2
3	Семинар на тему «Алгоритмы обучения многослойных нейронных сетей»	Компьютерная презентация	2
4	Практическое занятие «Алгоритм обратного распространения ошибки обучений нейронных сетей»	Разбор конкретных ситуаций	2
5	Практическое занятие «Описание алгоритма обучения нейронной сетевой для выявления атак на информационную систему»	Разбор конкретных ситуаций	2
Итого			10

6 Фонд оценочных средств для проведения промежуточной аттестации

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция
1	2
ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка

информационной безопасности	научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-2 - способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки	Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-5 - способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на

	<p>соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>УК-3 - готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач</p>	<p>Б1.Б.2 Иностранный язык Б1.В.ОД.1 Методология науки и образовательной деятельности Б1.В.ОД.2 Профессиональный иностранный язык Б1.В.ОД.3 Психология и педагогика Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>УК-6 - способность планировать и решать задачи собственного профессионального и личностного развития</p>	<p>Б1.Б.1 История и философия науки Б1.В.ОД.3 Психология и педагогика Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации ассиметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.1 Педагогическая практика Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>

Средствами промежуточного контроля успеваемости студентов являются защита практических заданий, опросы на практических занятиях по темам лекций. В конце семестра – зачет.

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её части)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
2	ОПК–2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	Знать: -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: - определять ее цель, задачи, разрабатывать гипотезу и определять способы ее проверки, Владеть: - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Знать: - основы культуры научного исследования, Уметь: - использовать и применять их в современных информационно-коммуникационных технологиях Владеть: - способностью к критическому анализу и оценке современных научных достижений	Знать: - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач Уметь: - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности Владеть: -организационными формами и методами проведения научных исследований;
3	ОПК–3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики объекта информатизации действующим стандартам, Владеть: - комплексной оценки	Знать: - методологические подходы применения нормативных документов при оценке защищённости объектов информатизации, Уметь: - выявлять недекларируемые угрозы объекту	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности Уметь: - вырабатывать методические рекомендации по реализации систем защиты Владеть:

		защищённости объекта информатизации	информатизации Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	-организационными формами и методами проведения научных исследований;
4	ПК-2 - способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки	Знать: -стандарты и нормативно-методические документы в области обеспечения информационной безопасности; Уметь: - сопоставлять характеристики нейросетевых систем действующим стандартам, Владеть: - комплексной оценки защищённости систем	Знать: - знание требований к защите информации определенного типа Уметь: - умение подобрать и обеспечить защиту информации Владеть: -владение современными средствами защиты информации;	Знать: - современных законов, стандартов, методов и технологий в области защиты информации; Уметь: - умение использовать современные программно-аппаратные средства защиты информации Владеть: - владение современными методами обеспечения защиты информации
5	ПК-5 - способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа	Знать: -стандарты и нормативно-методические документы в области обеспечения информационной безопасности; Уметь: - сопоставлять характеристики нейросетевых систем действующим стандартам, Владеть: - комплексной оценки защищённости систем	Знать: - знание требований к защите информации определенного типа Уметь: - умение подобрать и обеспечить защиту информации Владеть: -владение современными средствами защиты информации;	Знать: - современных законов, стандартов, методов и технологий в области защиты информации; Уметь: - умение использовать современные программно-аппаратные средства защиты информации Владеть: - владение современными методами обеспечения защиты информации
6	УК-3 - готовность участвовать в работе	Знать: -методологию	Знать: - основы культуры	Знать: - основные

	<p>российских и международных исследовательских коллективов по решению научных и научно-образовательных задач</p>	<p>исследовательской деятельности, основные проблемы в области информационной безопасности;</p> <p>Уметь:</p> <ul style="list-style-type: none"> - определять программу проведения исследований, <p>Владеть:</p> <ul style="list-style-type: none"> - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач 	<p>научного исследования в информационной безопасности,</p> <p>Уметь:</p> <ul style="list-style-type: none"> - использовать и применять их в современных информационно-коммуникационных технологиях <p>Владеть:</p> <ul style="list-style-type: none"> - способностью к критическому анализу результатов научного творчества 	<p>положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач</p> <p>Уметь:</p> <ul style="list-style-type: none"> - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности <p>Владеть:</p> <ul style="list-style-type: none"> - организационными формами и методами проведения научных исследований;
7	<p>УК-6 - способность планировать и решать задачи собственного профессионального и личностного развития</p>	<p>Знать:</p> <ul style="list-style-type: none"> - методологию исследовательской деятельности, основные проблемы в области информационной безопасности; <p>Уметь:</p> <ul style="list-style-type: none"> - определять программу проведения исследований, <p>Владеть:</p> <ul style="list-style-type: none"> - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач 	<p>Знать:</p> <ul style="list-style-type: none"> - основы культуры научного исследования в информационной безопасности, <p>Уметь:</p> <ul style="list-style-type: none"> - использовать и применять их в современных информационно-коммуникационных технологиях <p>Владеть:</p> <ul style="list-style-type: none"> - способностью к критическому анализу результатов научного творчества 	<p>Знать:</p> <ul style="list-style-type: none"> - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач <p>Уметь:</p> <ul style="list-style-type: none"> - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности <p>Владеть:</p> <ul style="list-style-type: none"> - организационными формами и методами проведения научных исследований;

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Введение в информационную безопасность Правовое обеспечение информационной безопасности	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Лекция с элементами проблемного изложения	См. МУ	Оценивая ответ, члены комиссии учитывают следующие <i>основные критерии</i> : – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и понимание предмета, которое подтверждается правильными ответами на дополнительные, уточняющие вопросы, заданные членами комиссии); – умение использовать теоретические знания при анализе конкретных проблем, ситуаций; – качество изложения материала, то есть обоснованность, четкость, логичность ответа, а также его полнота (то есть содержательность, не исключающая сжатости); – способность устанавливать внутри- и межпредметные связи, оригинальность и красота мышления, знакомство с дополнительной литературой и множество других факторов. <i>Критерии оценок:</i>
		ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Собеседование	См. МУ	
2	Организационное обеспечение информационной безопасности Технические средства и методы защиты информации	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция	Лекция с элементами проблемного изложения	См. МУ	
		ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Практическое занятие	Практическая работа	См. МУ	
3	Программно-аппаратные средства и методы обеспечения информационной безопасности	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3	Лекция Практическое занятие	Практическая работа		

		УК-6				Оценка <i>зачтено</i> – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и явлений, твёрдое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Предложенные в качестве самостоятельной работы формы работы (примерный план исследовательской деятельности; пробная рабочая программа) приняты без замечаний.
4	Введение в информационную безопасность Правовое обеспечение информационной безопасности	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Сообщение студента Практическая работа	См. МУ	
		ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие			
5	Организационное обеспечение информационной безопасности	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
6	Технические средства и методы защиты информации	ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-2 ОПК-3 ПК-2 ПК-5 УК-3 УК-6	Лекция Практическое занятие	Практическая работа		Оценка <i>не зачтено</i> – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение терминологией. Отсутствие выполненных самостоятельных дополнительных работ.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Список методических указаний, используемых в образовательном процессе, представлен в п. 7.2;

- Оценочные средства представлены в учебно-методическом комплексе дисциплины.

Текущая самостоятельная работа по данному курсу направлена на углубление и закрепление знаний, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;

- работа с рекомендованной литературой при подготовке к практическим занятиям;

- подготовка к зачету.

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

Контрольные вопросы для самостоятельной оценки качества освоения учебной дисциплины:

1. Мозг человека.
2. Механизмы обучения нейронных систем.
3. Правило обучения Хебба.
4. Принципы ассоциативного обучения.
5. Из истории развития искусственных нейронных сетей.
6. Различные подходы к классификации искусственных нейронных сетей.
7. Искусственный нейрон и принципы его функционирования.
8. Виды функций активации искусственного нейрона.
9. Решение задач классификации с помощью линейных нейронных сетей (геометрический способ).
10. Правило Хебба обучения нейронных сетей.
11. Обучение нейросети по Хеббу в матричной форме.
12. Недостатки правила Хебба обучения нейросети.
13. Алгоритм Розенблатта обучения нейронной сетей.
14. Правило Видроу-Хоффа обучения линейных нейронных сетей.
15. Описание алгоритма Видроу-Хоффа обучения нейронных сетей.
16. Выбор адаптивного шага обучения нейронной сети.
17. Обучение нейронной сети с помощью псевдообратных матриц.
18. Эквивалентность многослойной линейной нейронной сети однослойной.
19. Прогнозирование временных рядов линейными нейросетями.
20. Многослойные нейронные сети.
21. Теорема Колмогорова и возможности реализации непрерывных функций нейронными сетями.
22. Обоснование алгоритма обучения нейронной сетей обратным распространением ошибок.
23. Обобщенное дельта-правило обучения нейронных сетей.
24. Описание алгоритма обучения нейросетей обратным распространением ошибок.

25. Недостатки алгоритма обучения нейросетей обратным распространением ошибок.

26. Выбор адаптивного шага обучения в алгоритме обратного распространения ошибок.

27. Прогнозирование временных рядов многослойными нейронными сетями.

28. Использование логарифмической функции активации в нейронных сетях.

29. Рекуррентные нейронные сети.

30. Описание алгоритма обучения рекуррентной нейронной сети.

31. Самоорганизующиеся нейронные сети, сети Кохоннена.

32. Конкуренционное обучение нейронных сетей.

33. Работа нейросети на принципе конкуренции.

34. Векторный квантователь.

35. Контролируемое конкурентное обучение нейронных сетей.

36. Симметричные и асимметричные шифросистемы.

37. Различные протоколы распределения ключей.

38. Протокол распределения ключей на основе нейросетевого подхода.

39. Анализ надежности распределения ключей на основе нейросетевого подхода.

40. Нейросети как способ шифрования информации.

41. Стойкость системы шифрования на основе нейронных сетей.

42. Нейросетевые технологии распознавания атак на информационные системы.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) Основная литература:

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Текст]: монография / Н. И. Червяков [и др.]. - Москва: ФИЗМАТЛИТ, 2012. - 279 с.
2. Галушкин, А. И. Нейронные сети: основы теории [Текст] / А. И. Галушкин. – Москва : Горячая линия - Телеком, 2012. - 496 с.
3. Основы нейрокибернетики, генетические алгоритмы [Текст] : учебное пособие для студентов по специальности 230700, 230400, 010500, 060101, 060109 / Министерство образования и науки РФ, Юго-Западный университет ; ТулГУ ; сост. : О. Г. Павлов, Ю. А. Халин. - Тула : ТулГУ, 2014. - 103 с.
4. Таныгин, М. О. Программно-аппаратные системы защиты информации [Электронный ресурс] : учебное пособие / М. О. Таныгин ; Министерство образования и науки Российской Федерации, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2012. - 147 с.
5. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=276557>

б) Дополнительная литература:

1. Системы искусственного интеллекта. Практический курс [Текст] : учебное пособие / ред. И. Ф. Астахова. - М. : БИНОМ Лаборатория знаний, 2008. - 292 с.
2. Тимофеев, А. В. Адаптивное управление и интеллектуальный анализ информационных потоков в компьютерных сетях [Текст] : монография / А. В. Тимофеев ; Рос.акад. наук, С.-Петерб. ин-т информатики и автоматизации РАН. - Санкт-Петербург : Анатолия, 2012. - 278 с.
3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб: Издательство Политехнического университета, 2014. - 322 с. - Режим доступа : <http://biblioclub.ru>
4. Терехов, В. А. Нейросетевые системы управления [Текст] : учебное пособие для студентов вузов / В. А. Терехов, Д. В. Ефимов, И. Ю. Тюкин. - М. : Высшая школа, 2002. - 183 с.
5. Ярочкин, В.И. Информационная безопасность [Электронный ресурс]: учебник / В. И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с.

6. Голоко В. А. Нейронные сети: обучение, организация и применение [Текст] : учебное пособие для вузов / В. А. Голово, общ. ред. А. И. Галушкина. – М. : ИПРЖР, 2001. - 256 с.

7.2 Перечень методических указаний

1. Разработка систем принятия решений на основе нейронных сетей [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Интеллектуальные системы» для студентов специальности 09.04.01 «Информатика и вычислительная техника» / Юго-Зап. гос. ун-т ; сост. М. В. Бобырь . - Электрон. текстовые дан. (723 КБ). - Курск : ЮЗГУ, 2016. - 36 с.

2. Разработка нейронных сетей средствами MatLAB [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Интеллектуальные системы» для студентов специальности 09.04.01 «Информатика и вычислительная техника» / Юго-Зап. гос. ун-т ; сост. М. В. Бобырь. - Электрон. текстовые дан. (554 КБ). - Курск : ЮЗГУ, 2016. - 18 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Корпорация Microsoft [официальный сайт]. Режим доступа: <http://www.microsoft.com/>

2. Русскоязычный сайт сообщества Ubuntu [сайт]. Режим доступа: <http://ubuntu.ru/>

7.4 Перечень информационных технологий

3. MicrosoftOfficePowerPoint;
4. MicrosoftOfficeExcel;
5. ДиспетчеррисунковMicrosoftOffice:
6. MATLAB.

7.5 Другие учебно-методические материалы

1. Специальные требования и рекомендации по защите информации СТР-К, Государственная техническая комиссия при Президенте Российской Федерации. 2001.

2. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2002.

3. Гражданский кодекс РФ.

4. ФЗ № 24 от 20.02.95 «Об информации, информатизации и защите информации».

5. ФЗ № 15 от 20.01.95 «О связи».

6. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

8 Материально-техническое обеспечение дисциплины

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

8 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	2	3	4	5	6	7	8
1		4			1	01.09.17	Приказ ФГБОУ «Юго-Западный государственный университет» № 576 от 31.08.2017 г. « О внесении изменений в приказ №263 от 29.03.2017 г. « Об утверждении норм времени для расчета учебной и других видов работы»
2		8			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		18-19			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17

Приложение А

Темы рефератов

Примерный перечень тематик рефератов, подготавливаемых аспирантами.

1. Безопасность систем электронной почты. Правила пользования электронной почтой.
2. Безопасность Web-сервисов.
3. Вопросы обеспечения информационной безопасности корпоративных беспроводных сетей стандарта 802.11.
4. Выявление уязвимостей компьютерных сетей.
5. Персональные межсетевые экраны. Способы обхода межсетевых экранов.
6. Адаптивная безопасность сети: анализ защищенности и обнаружение атак.
7. Как работает сканер безопасности.
8. Организация защищенного подключения корпоративной сети к ГКС Интернет.
9. Система анализа защищенности InternetScanner.
10. Система анализа защищенности System Security Scanner.
11. Система обнаружения атак RealSecure.
12. Правовые основы деятельности по защите информации от НСД.
13. Инструментальные средства изучения защищенности информационных систем.
14. Методология оценки безопасности информационных технологий по общим критериям.
15. Информационная безопасность в современных системах управления базами данных.
16. Как защититься от программ-сканеров.
17. Безопасность сети: то, что должен знать каждый.
18. Анализ рынка средств защиты от копирования и взлома программных средств.
19. Обеспечение непрерывности деятельности организации в нештатных ситуациях. Составление Плана действий для Отдела Информационных технологий.
20. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак.
21. Информационная безопасность: экономические аспекты.
22. Системы обнаружения аномалий: новые идеи в защите информации.
23. Чем измерить безопасность Интернет?
24. Безопасность технологии GPRS.
25. Безопасность ноутбука.
26. Обзор программ-взломщиков паролей.
27. Безопасность программного обеспечения компьютерных систем.
28. Обзор профилей защиты на основе "Общих критериев".
29. Лазерный диск с нулевым треком как средство защиты от копирования.

- 30.Эффективность защиты информации.
- 31.Методики и технологии управления информационными рисками.
- 32.Безопасность систем с открытым кодом
- 33.Юридические аспекты борьбы со спамом
- 34.Методика построения корпоративной системы защиты информации
- 35.Оценка затрат компании на Информационную безопасность
- 36.Методические основы защиты информационных активов компании
- 37.Практическое применение международного стандарта информационной безопасности ISO 17799
- 38.Информационная безопасность и интересы бизнеса
- 39.Как определить источники угроз?
- 40.Анализ рынка средств защиты программного обеспечения от несанкционированного копирования
- 41.Компьютерные преступления (кто и как их совершает)
- 42.Современные факторы, влияющие на ЗИ.
- 43.Критерии, условия и принципы отнесения информации к защищаемой.
- 44.Состав и классификация носителей защищаемой информации.
- 45.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности, по собственникам и владельцам.
- 46.Каналы и методы НСД к конфиденциальной информации.
- 47.Направления, виды и особенности деятельности разведывательных служб по НСД к конфиденциальной информации.
- 48.Кадровое и ресурсное обеспечение ЗИ
- 49.Технологическое обеспечение ЗИ.
- 50.Назначение и структура систем ЗИ.