Приложение к ОПОП «Безопасность и этика искусственного интеллекта»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

РАБОЧАЯ ПРОГРАММА

дисциплины

«ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2023

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент Омский Государственный Технический Университет Сулавко А.Е.

заведующий кафедрой ”комплексная защита информации” Омский Государственный Технический Университет Ложников П.С.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ 02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	Иной
Обеспечивающая кафедра	ИК
Общая трудоемкость (ЗЕТ)	4
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	17
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	35
Самостоятельная работа, включая часы на контроль (академ. часов)	109
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»

Содержание дисциплины включает в себя изучение особенностей реализации зондирующих состязательных атак на нейросетевой искусственный интеллект (ИИ) с целью извлечения и интерпретации знаний, угроз защиты знаний ИИ от компрометации, архитектурных принципов построения ИИ на базе нейронных сетей, защищенных от подобного рода атак и угроз, нейросетевых моделей ИИ, исполняемых в защищенном режиме, а также методов и алгоритмов их синтеза и автоматического обучения на выборках малого или большого объема. Практические занятия ориентированы на проведение научно-исследовательской и опытно-конструкторской работы в области построения моделей и систем искусственного интеллекта, исполняемых в защищенном режиме, позволяющем защитить знания обученного искусственного интеллекта от компрометации при их обработке, хранении и передаче по каналам связи, а также защитить модель от ряда состязательных атак, зондирования и извлечения знаний.

SUBJECT SUMMARY

«PROTECTED EXECUTION OF ARTIFICIAL INTELLIGENCE»

The content of the discipline includes the study of the features of the implementation of probing adversarial attacks on neural network artificial intelligence (AI) in order to extract and interpret knowledge, threats to protect AI knowledge from compromise, architectural principles of building AI based on neural networks protected from this kind of attacks and threats, neural network AI models executed in a protected mode, as well as methods and algorithms for their synthesis and automatic training on small or large samples. Practical exercises are focused on conducting research and development work in the field of building models and systems of artificial intelligence, executed in a protected mode, which allows you to protect the

knowledge of trained artificial intelligence from compromise during their processing, storage and transmission through communication channels, as well as to protect the model from a series of adversarial attacks, probing and knowledge extraction.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Познакомить обучающихся с нейросетевыми архитектурами и моделями искусственного интеллекта, обладающими повышенной устойчивостью к компьютерным атакам, а также с принципами защищенного исполнения нейросетевых алгоритмов искусственного интеллекта в задачах классификации. Стать способным руководить проектами по созданию комплексных систем искусственного интеллекта и научиться исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта.

2. Изучить нейросетевые модели и архитектуры искусственного интеллекта, исполняемые в защищенном режиме, а также методы и алгоритмы их синтеза и автоматического обучения на выборках малого или большого объема. Сформировать и закрепить навыки проведения НИР и НИОКР в области построения моделей и систем искусственного интеллекта, исполняемых в защищенном режиме, позволяющем защитить знания обученного искусственного интеллекта от компрометации при их обработке, хранении и передаче по каналам связи, а также защитить модель от ряда состязательных атак, зондирования и извлечения знаний. Получить представление об особенностях реализации зондирующих состязательных атак на нейросетевой искусственный интеллект с целью извлечения и интерпретации знаний.

3. Знание принципов построения защищенных архитектур нейросетевого искусственного интеллекта для решения прикладных задач классификации образов; основных концепций, моделей и методов защищенного исполнения нейросетевых алгоритмов искусственного интеллекта. Знания единых стандартов в

области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения.

4. Умение проектировать архитектуры нейросетевого искусственного интеллекта для задач классификации образов, обладающего повышенной устойчивостью к компьютерным атакам; иллюстрировать и описывать научные результаты, полученные при разработке и тестировании эффективности нейросетевых алгоритмов искусственного интеллекта, исполняемых в защищенном режиме. Осуществлять руководство созданием комплексных систем искусственного интеллекта с применением новых методов и алгоритмов машинного обучения.

5. Навыки применения: методов и алгоритмов автоматического синтеза и обучения на малых выборках гибридных нейронных сетей и ансамблей классификаторов с учетом корреляционных матриц признаков; технологиями разработки и программной реализации нейросетевых моделей искусственного интеллекта, обладающего повышенной устойчивостью к компьютерным атакам.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Введение в нейронные сети»

2. «Машинное обучение»

3. «Доверенный искусственный интеллект»

4. «Криптография и криптографические протоколы»

и обеспечивает подготовку выпускной квалификационной работы.

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

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	Наименование компетенции/индикатора компетенции
ПК-23	Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта
ПК-23.3	*Разрабатывает единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также определяет критерии сопоставления программного обеспечения и критерии эталонных открытых тестовых сред (условий) в целях улучшения качества и эффективности программного обеспечения технологий и систем искусственного интеллекта*
ПК-27	Способен руководить проектами по созданию комплексных систем искусственного интеллекта
ПК-27.2	*Осуществляет руководство созданием комплексных систем искусственного интеллекта с применением новых методов и алгоритмов машинного обучения*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	ИКР, ач	СР, ач
1	Введение	2	2		5
2	Защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов	2	4		15
3	Защищенное исполнение нейросетевых алгоритмов на базе квадратичных нейронов	2	2		15
4	Защищенное исполнение нейросетевых алгоритмов на базе корреляционных нейронов	4	4		15
5	Защищенное исполнение гибридных нейросетевых алгоритмов	4	2		15
6	Заключение	3	3	1	44
	Итого, ач	17	17	1	109
	Из них ач на контроль	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4			

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение	Предмет дисциплины, её объём, содержание и связь с другими дисциплинами учебного плана. Компьютерные атаки на нейронные сети. Связь между защитой параметров обученной нейронной сети (знаний) и состязательными атаками. Атака «на решающий бит». Атака «ключ под ковриком». Состязательные атаки и зондирование нейронных сетей (атака «извлечения знаний»). Понятие преобразователя образов в код и защищенного исполнения нейросетевых алгоритмов. Области применения защищенного режима исполнения нейросетевых алгоритмов. Отлучение ИИ от принятия решений. Защита нейросетевых решающих правил на основе гомоморфного шифрования, классического шифрования и без использования шифрования. Повышение энтропии выходов преобразователя образов в код для противодействия атакам «извлечения знаний». Модели ИИ, способные к защищенному исполнению.

№ п/п	Наименование темы дисциплины	Содержание
2	Защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов	Атака извлечения знаний на примере нейросетевых преобразователей биометрия-ко (НПБК), обученного по ГОСТ Р 52633.5. НПБК –частный случай преобразователя образов в код. Энтропия выходов НПБК. Защищенные нейросетевые контейнеры (ЗНК), формируемые из параметров обученной неглубокой нейронной сети. Концепция ЗНК. Объединение нейронов в цепочки и шифрование параметров каждого нейрона с использованием ключа, формируемого на основании выходов предыдущих нейронов в цепочке путем применения обратимых и необратимых преобразований.
3	Защищенное исполнение нейросетевых алгоритмов на базе квадратичных нейронов	Плоское пространство признаков и мера Минковского. Искривление пространства признаков из-за взаимных корреляционных связей между признаками. Понятие спрямляющего пространства признаков. Проблема проклятья размерности. Обход проблемы проклятья размерности путем построения комитета (сети) частично связных квадратичных нейронов. Сети радиально-базисных функций. Сокрытие параметров распределения (статистических моментов) значений признаков после обучения сети квадратичных нейронов. Защищенное исполнение сетей квадратичных нейронов.
4	Защищенное исполнение нейросетевых алгоритмов на базе корреляционных нейронов	Понятие взаимной информации. Мера Байеса-Минковского. Точечная оценка корреляции. Мета-пространство признаков Байеса-Минковского и его построение с помощью специального отображения (на примере сгенерированных образов). Мета-пространства признаков Байеса-Минковского, не компрометирующие знания ИИ. Свойства мета-пространства признаков Байеса-Минковского. Защита знаний ИИ путем сокрытия статистических моментов признаков и дифференциальной конфиденциальности. Модели преобразователей образов в код на базе сетей корреляционных нейронов, алгоритмы их автоматического синтеза и обучения на малых выборках. Сокращение объема обучающей выборки путем перехода в мета-пространство признаков Байеса-Минковского. Стабилизация вычислений статистических моментов случайной величины. Повышение точности статистических оценок коэффициентов корреляции и гистограмм относительных частот на малых выборках.

№ п/п	Наименование темы дисциплины	Содержание
5	Защищенное исполнение гибридных нейросетевых алгоритмов	Модели гибридные нейронных сетей, состоящих из линейных, квадратичных и корреляционных нейронов. Синтез и автоматическое обучение гибридных нейронных сетей. Преимущества гибридных нейронных сетей. Объединение преобразователей образов в код (на базе любых видов нейронов) с глубокими нейронными сетями. Дрейф моделей ИИ в защищенном исполнении. Автоматическое переобучение (повторное обучение) преобразователей образов в код без переобучения (повторного обучения) глубокой нейронной сети. Построение экстракторов признаков с заданным законом распределения на базе нейронных сетей. Контроль распределения коэффициентов парной корреляции между признаками(балансировка внутренних корреляционных связей образов). Вариационные автокодировщики и их применение для извлечения признаков с нужными свойствами.
6	Заключение	Итоги курса. Перспективы развития нейросетевых моделей ИИ, способных к защищенному исполнению. О защищенном исполнении нейросетевых алгоритмов при построении сильного ИИ. Об объяснимости решений принимаемых ИИ в защищенном режиме исполнения.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Области применения защищенного режима исполнения нейросетевых алгоритмов. Обсуждение индивидуальных заданий	2
2. Оценка энтропии НПБК, обучаемого по ГОСТ Р 52633.5. Моделирование атаки извлечения знаний на НПБК	2
3. Защита нейросетевых контейнеров от извлечения знаний. Оценка энтропии НПБК в защищенном исполнении	1
4. Защищенный режим исполнения сетей квадратичных нейронов	2
5. Защищенный режим исполнения сетей корреляционных нейронов	4
6. Защищенный режим исполнения гибридных нейронных сетей	2
7. Защита ИДЗ	4
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание содержит постановку задачи, связанной с разработкой архитектуры интеллектуального программного модуля на базе нейросетевого ИИ, исполняемого в защищенном режиме. Оно выдается студенту на 1й неделе семестра. Каждое задание связано с определенной прикладной областью или сферой применения ИИ. Студент должен проанализировать материалы лекций, основную и дополнительную литературу, интернет источники, составить расширенную постановку задачи и согласовать ее с преподавателем. Требуется обдумать не только технические детали проекта программного модуля, но и потенциальную коммерциализуемость проекта.

Отчет по выполненному ИДЗ должен содержать аннотированное описание проведенной работы, включая следующие элементы:

- техническую и архитектурную документацию, объемом не менее 10 страниц, включая все функциональные схемы, графики, блок-схемы алгоритмов, формулы и описание модели ИИ, а также принципов защищенного исполнения нейросетевых алгоритмов. Дополнительным преимуществом, которое будет учитываться преподавателем при выставлении итоговой оценки, будет публикация научной статьи в журналах ВАК/РИНЦ/Scopus/Weeb of Science по теме ИДЗ;

- расширенное описание назначения продукта (проблема и решение). Дополнительным преимуществом, которое будет учитываться преподавателем при выставлении итоговой оценки, будет подготовка бизнес-модели продукта по шаб-

лону Остервальдера (при наличии такого желания у студента);

- презентация доклада (на 5-10 слайдов).

Отчет выполняется в электронном виде.

Примерные темы индивидуального домашнего задания (ИДЗ)

1. Система защищенного исполнения ИИ для нефтегазовой отрасли.
2. Система защищенного исполнения ИИ для оценки привлекательности инвестиций в сфере инноваций.
3. Система определения кредитоспособности заемщиков, устойчивая к дрейфу модели.
4. Система определения вторжений и DLP-система на базе ИИ.

Критерии оценки ИДЗ

1. Полнота представления материала. Наличие всех необходимых элементов и данных в отчете.
2. Понимание студентом материала, использованных методов и моделей, а также принципов их работы. Ясность изложения материала.
3. Корректность использования моделей и методов машинного обучения и защищенного исполнения нейросетевых алгоритмов искусственного интеллекта.

4.7 Доклад

Защита ИДЗ должна проходить в форме краткого доклада с презентацией (в формате питча). Регламент выступления 5 минут и 5 минут вопросы преподавателя.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками, научными публикациями и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Самостоятельное изучение студентами теоретических основ дисциплины обеспечено необходимыми учебно-методическими материалами (учебники, учебные пособия, конспект лекций и т.п.), выполненными в печатном или электронном виде. По каждой теме содержания рабочей программы могут быть предусмотрены индивидуальные домашние задания (расчетно-графические работы, доклады и т.п.).

Изучение студентами дисциплины сопровождается проведением регулярных консультаций преподавателей, обеспечивающих практические занятия по

дисциплине, за счет бюджета времени, отводимого на консультации (внеаудиторные занятия, относящиеся к разделу «Самостоятельные часы для изучения дисциплины»).

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	10
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	10
Самостоятельное изучение разделов дисциплины	0
Выполнение домашних заданий, домашних контрольных работ	20
Подготовка к лабораторным работам, к практическим и семинарским занятиям	0
Подготовка к контрольным работам, коллоквиумам	0
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	14
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	20
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	109

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Николенко С. Глубокое обучение [Электронный ресурс] / С. Николенко, А. Кадурин, Е. Архангельская, 2019. -480 с.	неогр.
Дополнительная литература		
1	Чио К. Машинное обучение и безопасность [Электронный ресурс] : руководство / К. Чио, Д. Фримэн, 2020. -388 с.	неогр.
2	Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных [Электронный ресурс], 2015. -400 с.	неогр.
3	Соколов, Алексей Иванович. Нейронные сети и нейродинамические системы [Электронный ресурс] : электрон. учеб. изд. / А. И. Соколов, С. С. Чистякова, 2016. -1 эл. опт. диск (CD-ROM)	неогр.

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «Издательство LEM», 2014 – 144 с.http://lib.tarsu.kz/rus/all.doc/Elektron_res/Axmetov_Texnologia%20neironnix%20setei.pdf
2	Иванов А.И., СулавкоА.Е. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила// Пенза –2020 г. Издательство «ПГУ» –48 с. Тираж 300 экз. ISBN978-5-907364-02-8 –URL:https://tsib.pnzgu.ru/files/tsib.pnzgu.ru/ivanov_sulavko_preprint_2020_ispolzsetkorrelneyron.pdf
3	Иванов, А. И., Золотарева Т. А. Искусственный интеллект в защищенном исполнении: синтез статистико-нейросетевых автоматов многокритериальной проверки гипотезы независимости малых выборок биометрических данных : препринт. –Пенза : Изд-во ПГУ, 2020. –104 с. –URL:https://tsib.pnzgu.ru/files/tsib.pnzgu.ru/ivanov_zolotareva_preprint_2020_iskusstvintellekt.pdf

№ п/п	Электронный адрес
4	Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Монография. Пенза –2016 г. Издательство АО «Пензенский научно-исследовательский электротехнический институт» (ОА «ПНИЭИ») –133 с.–URL:https://tsib.pnzgu.ru/files/tsib.pnzgu.ru/ivanov_mnogomernaya_monografiya.pdf
5	Наборы данныхhttp://aiconstructor.ru/page14247028.html
6	ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификацииhttps://docs.cntd.ru/document/1200048922
7	ГОСТ Р 52633.1-2009 Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификацииhttps://docs.cntd.ru/document/1200079555
8	ГОСТ Р 52633.2-2010 Защита информации. Техника защиты информации. Требования к формированию синтетических и биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификацииhttps://docs.cntd.ru/document/1200081163
9	ГОСТ Р 52633.3-2011 Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подборahttps://docs.cntd.ru/document/1200088765
10	ГОСТ Р 52633.4-2011 Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия -код доступаhttps://docs.cntd.ru/document/1200093473
11	ГОСТ Р 52633.5-2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступаhttps://docs.cntd.ru/document/1200088764
12	ГОСТ Р 52633.6-2012 Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу ”Свой”https://docs.cntd.ru/document/1200095360

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=7827

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Защищенное исполнение искусственного интеллекта» предусмотрены следующие формы промежуточной аттестации: экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Студент продемонстрировал существенные пробелы в знаниях основного учебного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий.
Удовлетворительно	Студент продемонстрировал знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, обладает необходимыми знаниями, но допустил неточности в ответах на аттестационном испытании и при выполнении учебных заданий.
Хорошо	Студент продемонстрировал полное знание учебного материала, успешно выполнил предусмотренные программой задачи, освоил основную рекомендованную литературу, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.
Отлично	Студент продемонстрировал всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоил основную литературу и ознакомился с дополнительной литературой, рекомендованной рабочей программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебного материала.

Особенности допуска

Для допуска к экзамену студент должен успешно выполнить и защитить ИДЗ, пройти тестирование, проводимое на 7 неделе, получив оценку «удовлетворительно» или выше.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	Подходы к построению защищенного режима исполнения нейросетевых алгоритмов
2	Требования к энтропии выходов преобразователей образов в код
3	Отображения для перехода в спремляющее мета-пространство признаков Байеса-Минковского
4	Понятие взаимной информации. Оценка информативности корреляционных связей между признаками
5	Принцип работы корреляционных нейронов
6	Принцип работы квадратичных нейронов

Вариант экзаменационного теста

Экзаменационный тест содержит 10 вопросов из разных тем курса. Для получения оценки «удовлетворительно» необходимо дать правильные ответы на 60% или более тестовых вопросов, «хорошо» - на 75% или более, «отлично» - на 90% или более.

Примерные вопросы и варианты ответов для тестов при проведении текущего контроля

Вопрос

По какому критерию следует судить о близости синтетических образов «Чужих» к истинному образу «Свой» при зондировании модели неглубокой нейронной сети, обученной по ГОСТ Р 52633.5, с целью извлечения знаний из нейросетевого контейнера?

Варианты ответа:

1. Повышение стабильности кодов, генерируемых нейронной сетью (нейросетевым преобразователем образов в код), при поступлении на ее входы примеров класса образов «Чужой»;

2. Повышение информационной энтропии кодов, генерируемых нейронной сетью (нейросетевым преобразователем образов в код), при поступлении на ее входы примеров класса образов «Чужой»;

3. Повышение вероятностей ошибочных решений нейронной сети.

Вопрос:

Какой тип нейронов позволяет наиболее эффективно обрабатывать векторы признаков с высоким уровнем взаимной корреляционной зависимости?

Варианты ответа:

1. Линейные (на основе взвешенного суммирования);

2. Квадратичные (на основе меры Евклида);

3. Корреляционные (на основе меры близости Байеса-Минковского).

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Введение	
2		Тест
3	Защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов	
4		
5		Тест
6	Защищенное исполнение нейросетевых алгоритмов на базе квадратичных нейронов	
7		Тест
8	Защищенное исполнение нейросетевых алгоритмов на базе корреляционных нейронов	
9		
10		
11		ИДЗ / ИДРГЗ / ИДРЗ
12	Защищенное исполнение гибридных нейросетевых алгоритмов	
13		
14		ИДЗ / ИДРГЗ / ИДРЗ
15	Заключение	
16		
17		ИДЗ / ИДРГЗ / ИДРЗ

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя:

- контроль посещаемости (не менее 80 % занятий);

- проведение дискуссий и обсуждений ИДЗ в конце каждой лекции, активное участие в которых может учитываться преподавателем, как один из способов текущего контроля на лекционных занятиях.

на практических (семинарских) занятиях

Текущий контроль включает в себя:

- контроль посещаемости (не менее 80 % занятий);

- устный опрос по теме практического занятия;

- выполнение теста. Тест состоит из 10 тестовых заданий. Для получения

оценки «удовлетворительно» необходимо дать правильные ответы на 60% или более тестовых вопросов, «хорошо» - на 75% или более, «отлично» - на 90% или более.

- выполнение и защита ИДЗ (с 11-й по 17-ю неделю).

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	1) Количество посадочных мест – в соответствии с контингентом, 2) рабочее место преподавателя, персональный компьютер IBM, совместимый Pentium или выше, проектор, экран/интерактивная панель, меловая/маркерная доска.	1) Windows 7 и выше; 2) Microsoft Office 2007 и выше
Практические занятия	Аудитория	1) Количество посадочных мест, оборудованных компьютерами IBM совместимыми Pentium или выше, – в соответствии с контингентом, 2) рабочее место преподавателя, персональный компьютер IBM совместимый Pentium или выше, проектор, экран/интерактивная панель, меловая/маркерная доска.	1) Windows 10; 2) Microsoft Office 2007 и выше; 3) Python 3.6; 4) keras 2.2.5; 5) tensorfow 1.6.0; 6) protobuf 3.6.0; 7) NET Core 3.0 или выше.
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows 10; 2) Microsoft Office 2007 и выше; 3) Python 3.6; 4) keras 2.2.5; 5) tensorfow 1.6.0; 6) protobuf 3.6.0; 7) NET Core 3.0 или выше.

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА
1	23.12.2021	Внесены изменения в компетентностную модель образовательной программы, на основании письма Минобрнауки России от 21.12.2021 № МН-5/22720	23.12.2021 №9	доцент Омский Государственный Технический Университет, А.Е. Сулавко; заведующий кафедрой ”комплексная защита информации” Омский Государственный Технический Университет, П.С. Ложников	

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА
2	18.05.2023	Программа актуальна, изменения не требуются.	18.05.2023 г., протокол заседания УМК № 4	доцент Омский Государственный Технический Университет, А.Е. Сулавко; заведующий кафедрой ”комплексная защита информации” Омский Государственный Технический Университет, П.С. Ложников	