АННОТАЦИИ РАБОЧИХ ПРОГРАММ

образовательной программы подготовки магистров

«Безопасность и этика искусственного интеллекта»

по направлению

09.04.01 «Информатика и вычислительная техника»

«Анализ данных в искусственном интеллекте»

Освещаемые в курсе теоретические и прикладные вопросы полезны для студентов, специализирующихся в области управления и информационных технологий в технических системах, компьютерного и математического моделирования. В курсе даются основы Data Science, включающие вопросы сбора, хранения и подготовки данных (выявление аномалий в сырых данных, очистка данных от шума, дополнение данных, заполнение (удаление) пропущенных значений), классификации и кластеризации, поиска ассоциативных правил, интерполяции, экстраполяции и аппроксимации, корреляционного и регрессионного анализа, искусственного интеллекта и машинного обучения, нейронных сетей, сверточных нейронных сетей. Кроме того, в курсе рассматривается современная вычислительная база в контексте решения задач Data Science (CUDA, GPU, FPGA, SoC). Уделяется внимание решению практических задач с использованием современных программно-аппаратных средств (MATLAB, Python, R, GPU).

«Аналитическая обработка данных в задачах информационной безопасности»

Дисциплина посвящена изучению безопасности личности в цифровом пространстве, разведке в информационном пространстве, информационных войнах и применению больших объемов данных в задачах информационной безопасности. В рамках данной дисциплины рассматриваются основные подходы к сбору больших объемов информации из открытых источников, их накоплению, обработке и анализу. Дисциплина формирует знания студентов

о современных технологиях анализа цифрового следа личности, дает понимание природы утечек информации и применения больших данных в SIEM (также необходимости самих SIEM). Также дисциплина формирует умения и навыки работы с самыми современными технологиями контейнеризации и их аспектами безопасности, нереляционными и графовыми базами данных, стеком Apache Hadoop и Apache NiFi (для хранения и обработки больших объемов данных), технологиями машинного обучения и графовыми нейронными сетями, а также применения данных технологий в информационной безопасности.

«Аппаратно-программные средства защиты информации в компьютерных системах»

Дисциплина формирует знания, умения и навыки необходимые для защиты информации в компьютерных системах с применением современных аппаратно-программных средств защиты информации. В рамках дисциплины изучаются следующие основные темы: Основные понятия программно-аппаратной защиты информации, принципы её построения. Задачи программно-аппаратной защиты информации. Нормативные документы, посвященные вопросам применения программно-аппаратных средств защиты информации. Методы и средства защиты информации от НСД. Идентификация и аутентификация пользователей. Разграничение доступа. Доверенная загрузка. Изолированная программная среда. Программно-аппаратные механизмы защиты ОС специального назначения. Механизмы защиты сертифицированных антивирусных средств. Практические часть курса, в составе практических работ, нацелена на закрепление материала и получение навыков по настройке аппаратно-программных средств защиты информации по определенным правилам, установленным нормативными или нормативно-методическими документами.

«Архитектура параллельных вычислительных систем»

Дисциплина посвящена методам организации и средствам параллельных и распределенных научных вычислений на основе применения

современных методов и средств современного программного и аппаратного обеспечения. В процессе обучения предполагается сформировать у студентов практические навыки работы с высокопроизводительными вычислительными системами.

«Атаки на нейронные сети»

В дисциплине рассматриваются теоретические основы атак на нейронные сети с целью обмана моделей с помощью специально подобранных входных данных. В курсе используются библиотеки построения нейронных сетей PyTorch и TensorFlow, а также библиотека генерации атак FoolBox.

«Введение в нейронные сети»

Содержание дисциплины включает в себя изучение основ теории искусственных нейронных сетей, их применение в решении задачи предсказания, а также обзор вспомогательных технологий, используемых в тренировке глубоких нейронных сетей (дропаут, регуляризация, нормализация и т.д.).

«ГИА»

Государственная итоговая аттестация включает в себя защиту выпускной квалификационной работы. Государственная итоговая аттестация является заключительным этапом освоения основной образовательной программы. В ходе государственной итоговой аттестации устанавливается уровень подготовки выпускника высшего учебного заведения к выполнению профессиональных задач и соответствия его подготовки требованиям стандарта.

«Доверенный искусственный интеллект»

Содержание дисциплины включает в себя изучение проблем обеспечения доверия к искусственному интеллекту (ИИ) и подходов к их решению, а также свойств, качеств доверенного искусственного интеллекта и понятий, непосредственно связанных с доверием к ИИ, таких как управление рисками ИИ, робастность ИИ, объяснимость ИИ, функциональная безопасность ИИ. Практические занятия ориентированы на проведение аналитической работы, развитие способностей к проведению аналитико-синтетических исследований научных публикаций и технических статей на примере тематики обеспечения доверия к ИИ.

«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.

«Иностранный язык»

Цель курса — обучение практическому владению иностранным языком (английским, немецким, французским), критерием которого является умение пользоваться наиболее употребительными языковыми средствами в основных видах речевой деятельности: говорение, аудирование, чтение и письмо. Задача курса – уметь общаться в большинстве ситуаций, которые могут возникнуть в повседневной и профессиональной деятельности. По структуре курс делится на следующие аспекты (модули): разговорная практика и аудирование, чтение, письменная практика, практика перевода и практическая грамматика, которые различаются тематикой и лексическим составом учебного и информационного материалов, при этом связаны между собой необходимостью систематического совершенствования всех четырех языковых умений и основных грамматических тем.

«Интеллектуальные системы»

Рассматриваются основные понятия теории интеллектуальных систем; средства языка логического программирования для разработки интеллектуальных систем: рекурсивные программы, решение логических задач с использованием структур данных – списков и деревьев; интерактивная визуальная среда логического программирования Visual Prolog; основы построения и использования экспертных систем; методы планирования действий в интеллектуальных системах; теоретические и практические основы организации обучения в интеллектуальных системах; методы поиска в условиях противодействия.

Лабораторные работы ориентированы на изучение языка логического программирования в среде Visual Prolog, программирование с использованием структур данных списки и деревья, разработку экспертной системы на языке логического программирования, исследование моделей планирования в интеллектуальных системах.

«Криптография и криптографические протоколы»

Данная дисциплина формирует знания и умения, необходимые для разработки криптографических алгоритмов и криптографических протоколов, а также формирует компетенции для анализа устойчивости криптопроколов/криптоалгоритмов к различного вида криптоатакам.

В рамках дисциплины изучаются следующие основные темы: основные криптоалгоритмы, принципы построения криптопротоколов, алгоритмы создания и проверки электронной цифровой подписи, гибридные криптосистемы, наиболее применяемые протоколы, используемые для защиты информации в интернете, протоколы видео конференций на примере WhatsApp, принципы построения криптопротоколов.

Практические часть курса, в составе практических работ нацелена на изучение принципов работы криптоалгоритмов/криптопротоколов и анализ их криптостойкости.

«Математические основания информатики»

Дисциплина «Математические основания информатики» относится к обязательной части учебного плана магистратуры по направлению «Информатика и вычислительная техника». Она является органическим продолжением дисциплин «Дискретная математика» и «Математическая логика и теория алгоритмов», изучаемых по учебным планам бакалавров. Цель дисциплины – поднять математическую культуру студентов, овладеть основными моделями и методами компьютерной математики. Дисциплина состоит из следующих разделов: функции конечнозначной логики; прикладная логика.

«Машинное обучение»

Содержание дисциплины включает в себя изучение основных моделей машинного обучения: методов поиска выбросов, метрических и логических методов обработки данных (метод ближайшего соседа, деревья решений,

линейная регрессия и т.д.). Практические занятия ориентированы на исследование методов обработки данных и оценке качества построенных моделей.

«Машинное обучение в приложениях биометрии»

Содержание дисциплины включает в себя изучение подходов, методов и алгоритмов для реализации процедур биометрической идентификации и аутентификации, а также моделей классификаторов и алгоритмов машинного обучения на малых выборках биометрических данных. Практические занятия ориентированы на применение методов машинного обучения и распознавания образов при решении сложных научно-технических проблем,связанных с анализом биометрических данных и информационной безопасностью, а также развитие творческих подходов и закрепление знаний в области науки о данных и машинного обучения на примере решения задач классификации биометрических образов.

«Методология научного познания»

Дисциплина «Методология научного познания» входит в обязательную часть общенаучного цикла подготовки магистров. Целью изучения дисциплины является ознакомление магистрантов со структурой научного знания, с методами научного исследования, с функциями научных теорий и законов; расширение их мировоззренческого кругозора; выработка представлений о критериях научности и о требованиях, которым должно отвечать научное исследование и его результаты

«Основы построения защищенных компьютерных сетей»

Дисциплина посвящена основным принципам построения защищенных телекоммуникаций. В содержание дисциплины входят основные направления обеспечения защиты компьютерных сетей: обнаружение компьютерных атак, межсетевое экранирование, организация виртуальных частных сетей,

технологии предотвращения вторжений, основанные на методах интеллектуального аудита информационной безопасности. В ходе изучения студенты получают знания о базовых принципах обеспечения защиты информации при ее передаче и приобретают навыки, необходимые для практического построения и администрирования защищенных компьютерных сетей с применением современных средств защиты информации. Полученные знания позволяют правильно ориентироваться в многообразии выпускаемых и предлагаемых программно-аппаратных средств сетевой защиты.

«Основы предпринимательства»

Целью освоения дисциплины «Основы предпринимательства» является освоение теории и практики предпринимательства в Российской Федерации.

Изучение основ создания собственного дела, приобретение навыков адаптации теоретических знаний к российской практике предпринимательства, изучение организации процессов предпринимательской деятельности и оформление их в бизнес-план. В ходе изучения дисциплины разбираются возможные проблемы и трудности, с которыми сталкивается предприниматель на начальном этапе. Дисциплина базируется на основе действующего законодательства Российской Федерации в области регулирования процессов предпринимательской деятельности и защиты интеллектуальной собственности.

В результате изучения дисциплины формируются практические навыки по открытию собственного дела, по решению задач текущей предпринимательской деятельности, по поиску новых идей и ресурсов для развития бизнеса, по регистрации прав на интеллектуальную собственность.

«Построение и оптимизация алгоритмов»

Дисциплина относится к обязательной части учебного плана магистратуры по направлению «Информатика и вычислительная техника».

Она опирается на дисциплину «Математические основания информатики», изучаемую в 1 семестре и на дисциплины учебного плана бакалавров. Цель дисциплины овладеть основными методами построения, анализа и оптимизации алгоритмов. Дисциплина состоит из следующих разделов: методы построения алгоритмов; теория сложности алгоритмов; оптимизация алгоритмов.

«Производственная практика (научно-исследовательская работа)»

Производственная практика проводится в целях получения профессиональных умений и опыта профессиональной деятельности, в том числе осуществления научно-исследовательской деятельности, участия в научно-практических конференциях, публикации научных результатов исследований.

«Производственная практика (преддипломная практика)»

Преддипломная практика проводится для подготовки выпускной квалификационной работы. Во время прохождения преддипломной практики обучающийся должен довести до финального результата исследования по теме своей выпускной квалификационной работы, оформить пояснительную записку к выпускной квалификационной работе и презентацию.

«Производственная практика (технологическая (проектно-технологическая) практика)»

Производственная практика (технологическая (проектно-технологическая) практика), распределенная в семестре, обеспечивает приобретение теоретических знаний и практических навыков в области: проведения самостоятельной проектной работы; закрепления знаний по изучаемым дисциплинам; приобретение опыта практической деятельности при построении и использовании интегрированных систем управления качеством в организациях. Производственная практика (технологическая

(проектно-технологическая) практика) проводится с целью формирования производственно-технологических компетенций для успешной будущей профессиональной деятельности.

«Русский язык как иностранный»

Дисциплина ориентирована на обучение иностранных магистрантов нефилологических специальностей, имеющих диплом бакалавра Российских вузов и владеющих русским языком на уровне ТРКИ-2. Содержание программы составляют требования к уровню владения языком в различных видах речевой деятельности, а также языковой и речевой материал. Освоение программы позволит иностранным учащимся удовлетворить необходимые коммуникативные потребности прежде всего в учебной и социально-культурной сферах общения, создаст базу для успешного усвоения специальных дисциплин и, в конечном итоге, успешной защиты ВКР. Курс русского языка для магистрантов призван обеспечить формирование коммуникативной компетенции выпускника на уровне, достаточном для квалифицированного осуществления им профессиональной деятельности на русском языке. Обучение осуществляется на материале общенаучных, профильных, страноведческих, литературно-художественных и общественно-политических текстов.

«Теория информации и теория кодирования»

Дисциплина формирует знания и умения, необходимые для понимания работы и разработки кодов исправляющих ошибки. В рамках дисциплины изучаются следующие основные темы: основы теории информации, линейные и нелинейные коды, их сферы применимости, AMD коды, канальное кодирование, сферы применимости кодов исправляющих ошибки. Практические часть курса, в составе практических работ, нацелена на реализацию изученных кодов, и их применение.

«Технология разработки программного обеспечения»

Дисциплина обеспечивает формирование знаний и умений в сфере современных технологий командной разработки ПО. Рассматриваются различные модели жизненного цикла разработки ПО, интегрированная модель зрелости предприятия (CMMI) и ее ключевые области.

Проводится обзор современных стандартов, методологий, документированных процессов и сред разработки ПО: Rational Unified Process, Microsoft Solutions Framework и Team Foundation Server, гибкие (agile) методологии разработки. Рассматриваются вопросы построения проектного процесса, распределение ролей в проекте, методы планирования и отслеживания работ, контроля качества, управления рисками. Полученные знания закрепляются при выполнении курсового проекта по разработке ПО. Обязательным является использование современных средств разработки (Java / .Net), систем версионного контроля, средств управления конфигурацией, отслеживания дефектов, автоматизации тестирования и контроля качества кода. Еженедельная публичная отчетность команд с демонстрацией проектных метрик и прототипов обеспечивает высокий уровень соревновательности.

«Управление проектированием информационных систем»

Дисциплина обеспечивает теоретическую и практическую подготовку в области управления проектированием архитектуры и программного обеспечения информационных систем (ИС). Программа дисциплины включает изучение основных направлений управления проектированием программного обеспечения ИС. В рамках дисциплины рассматриваются понятие и модели жизненного цикла программного обеспечения, унифицированный и экстремальный процессы разработки программных изделий, планирование и управление конфигурацией программного проекта, стандарты и обеспечение качества программных изделий, вопросы сопровождения программных изделий.

«Учебная практика (технологическая (проектно-технологическая) практика)»

Учебная практика проводится в целях получения первичных профессиональных умений и навыков и включает в себя, во-первых, работу по определению темы научно-исследовательской работы, которая будет выполняться в течение производственной практики следующих семестров, во-вторых, практику по получению первичных профессиональных умений и навыков в лабораториях кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».

«Этика и правовые проблемы искусственного интеллекта»

Стремительный рост технологий на базе искусственного интеллекта (ИИ) может произвести революцию в мире и принести множество преимуществ обществу, организациям и отдельным лицам. Однако такой рост может иметь существенные риски. Лица, принимающие участие в жизненном цикле систем на базе ИИ (акторы ИИ), должны знать об этических и правовых проблемах, которые влечет за собой развитие ИИ. Эти проблемы весьма разнообразны – от нарушений конфиденциальности и безопасности сведений ограниченного доступа до дискриминации лиц по признакам расовой, национальной принадлежности, политических взглядов и др. Вред, причиняемый акторами ИИ, может быть как неумышленным так и намеренным. Во втором случае целью также может быть причинение вреда окружающей среде, жизни и здоровью или имуществу граждан и юридических лиц. Поскольку законодательство и нормативные акты часто отстают от темпов демократизации ИИ, существует потребность в разработке этических рамок, принципов ИИ, инструментов и методов снижения рисков, анализа и обнаружения угроз, а также передовых методов тестирования и оценки воздействия ИИ.

Настоящая дисциплина направлена на изучение общих этических принципов использования технологий ИИ с помощью междисциплинарного

и межотраслевого подхода, включая всех участников на всех этапах цепочки жизненного цикла систем ИИ, а также соблюдения действующих и разработанных в случае необходимости нормативно-правовых актов, международных договоров и соглашений, применимых к вопросам обеспечения прав и свобод граждан в контексте использования информационных технологий и ИИ.