Федеральное государственное учреждение
«Федеральный исследовательский центр
«Информатика и управление»
Российской академии наук»
(ФИЦ ИУ РАН)

Россия, 119333, г. Москва, ул. Вавилова, д .44, корп. 2
Тел. 8 (499) 135-62-60, факс 8 (495) 930-45-05
E-mail: frccsc@frccsc.ru http://www.frccsc.ru

От _____№ _____

На № _____

РЕЦЕНЗИЯ
на магистерскую образовательную программу «Искусственный интеллект в кибербезопасности» по направлению подготовки 01.04.02 «Прикладная математика и информатика» (форма обучения: очная)

Обоснование актуальности

Искусственный интеллект позволяет эффективнее решать задачи по обнаружению киберугроз и защите устройств и систем от атак, что имеет важность не только для отдельных лиц и компаний, но и национальной безопасности.

Магистерская программа «Искусственный интеллект в кибербезопасности» является уникальной не только в России, но и в мире и направлена на подготовку математиков и программистов для решения задач, связанных с безопасностью, робастностью и надежностью систем, построенных с использованием методов искусственного интеллекта и машинного обучения. Специалисты высшей квалификации в сфере применения искусственного интеллекта для обеспечения кибербезопасности востребованы в научно-исследовательских институтах, IT-компаниях, банках, высших, средних, средних специальных учебных заведениях и государственных структурах.

Поэтому разработка и реализация магистерской программы на факультете вычислительной математики и кибернетики МГУ им. М.В. Ломоносова актуальна.

Цели разработки образовательной программы

Основная цель магистерской программы – подготовка высококвалифицированных специалистов, сочетающих глубокие знания криптографии, математики и программирования, которые будут способны обеспечить безопасность информационной системы.

Характеристика и оценка разработанной образовательной программы

Программа направлена на получение компетенций в синтезе и анализе криптосистем с открытым и секретными ключами для построения эффективной системы информационной безопасности.

Важная особенность представленной образовательной программы состоит в том, что в духе времени она реализует идеи компетентностного подхода, которому присущ перенос акцента с преподавателя и содержания дисциплины («подход, центрированный на преподавателе») на студента и ожидаемые результаты образования («подход, центрированный на студенте»). Разработаны карты компетенций: общекультурных, общепрофессиональных и профессиональных для данной магистерской программы, такие как. Набор компетенций также включает специализированные компетенции, отражающие запросы профессионального сообщества.

В дисциплинах программы рассматриваются основы суперкомпьютерного моделирования, вопросы тестирования информационной безопасности систем и различные разделы криптографии. Набор дисциплин освещает основные методы и технологии, используемые в защите от киберугроз. В достижении целевых компетенций магистрантам помогают курсы «Тестирование безопасности компьютерных систем», «Суперкомпьютерное моделирование и технологии», «Математическая криптография», которые содержат актуальные, новейшие сведения изучаемой области знания.

Набор дисциплин включает сбалансированную теоретическую и практическую подготовку специалиста в посторенние системы информационной безопасности Стоит отметить ценность практической составляющей курса, включающий дисциплины по созданию эффективной системы защиты безопасности, например «Синтез и анализ криптосистемы с открытым ключом», описывающей стойкость данных систем и практическую реализацию их самих и атак на них и дисциплины.

Оценка технологий обучения

Рецензируемая образовательная программа подготовки магистров близка к оптимуму, когда сочетает как традиционные, так и современные (инновационные) образовательные технологии: лекции, семинары, практические занятия, интерактивные лекции, лекции с применением мультимедийных средств, проблемные лекции, лекции-дискуссии, занятия с применением затрудняющих условий, компьютерные симуляции, компьютерное тестирование, групповые дискуссии, тренинги, разбор конкретных ситуаций и другие. При проведении занятий предусматривается участие ведущих специалистов в соответствующей области.

Таким образом, многосторонний анализ показал, что представленная основная образовательная программа подготовки «Искусственный интеллект в кибербезопасности»

по направлению подготовки 01.04.02 «Прикладная математика и информатика» логично выстроена и достаточна для обеспечения образовательного процесса по достижению заявленных компетенций выпускника. Программа достаточна для формирования специалиста, имеющего фундаментальную подготовку в области построения систем информационной защиты и обеспечения кибербезопасности, имеющего важные практические компетенции в области программирования, математического моделирования, готового к успешной карьере в сфере информационной технологий.

Магистерскую программу «Искусственный интеллект в кибербезопасности» можно охарактеризовать как уникальную и инновационную, разработанную на основании мирового опыта и ведущих тенденций развития систем применения искусственного интеллекта и обеспечения кибербезопасности. Программа соответствует отечественным и мировым тенденциям и рекомендована к реализации в рамках учреждений высшего образования.

Ученый секретарь,
д-р техн. наук

В.Н.Захаров

«14» октября 2021 г.