Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
декан факультета вычислительной
математики и кибернетики

_____/И.А. Соколов /
«__4__» ____октября_____2021г.

АННОТАЦИЯ МАГИСТЕРСКОЙ ПРОГРАММЫ

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

01.04.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Искусственный интеллект в кибербезопасности

Форма обучения:

очная

Программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №__7__, от 29 сентября 2021 года)

Москва 2021

Направления подготовки

Направление подготовки: 01.04.02 «Прикладная математика и информатика»

Также указанный профиль может быть рекомендован для реализации в следующих направлениях подготовки:

02.03.01 Математика и компьютерные науки

090301 Информатика и вычислительная техника

090303 Прикладная информатика

090304 Программная инженерия

01.03.04 Прикладная математика

02.03.03 Математическое обеспечение и администрирование информационных систем

Актуальность магистерской программы

Развитие современного общества пришло к тому, что многие сферы человеческой деятельности были автоматизированы с помощью компьютеров. Настоящий мир совершенно не мыслим без использования информационных технологий. Электронные платежные системы, интернет-магазины, оказание государственных услуг в электронном виде, электронное правительство, банковские карточки и т.д. – все это удобные атрибуты современного общества. Кроме того, в большинстве современных интернет-технологий используются системы искусственного интеллекта, а также различные интеллектуальные методы обработки больших данных.

За последнее десятилетие проблема защиты информации, благодаря всё пронизывающей компьютеризации, стало по настоящему «народной». Если ещё каких-то 30 лет назад проблемой защиты информации были обеспокоены только государства, то сейчас так или иначе это касается каждого живущего на планете Земля. Облик защиты информации за эти годы изменился. Если раньше основной целью защиты информации было обеспечение конфиденциальности, то есть обеспечение того, что никто

«чужой» не узнает некоторой важной информации, то, с тех пор как информация стала товаром, к этой цели добавились обеспечение целостности (неизменности) информации, а также обеспечение ее доступности. Большое пространство для злоумышленников открывают новые технологии искусственного интеллекта, для которых были разработаны методы нарушения их устойчивости.

В последнее время в мире возросло число преступлений в компьютерной сфере или, так называемых, киберпреступлений. Эффективное противостояние им, обеспечение безопасной жизни каждого человека и государства в целом – вот глобальная задача защиты информации сегодня.

Содержание магистерской программы “Искусственный интеллект в кибербезопасности” полностью отражает современную тенденцию в применении технологии искусственного интеллекта для построения новых систем кибербезопасности, а также в разработке новых методов и подходов к обеспечению безопасности самой технологии искусственного интеллекта. Содержание программы находится на стыке различных областей знания. Несомненно, основу здесь составляет математика. Слушатели программы познакомятся с различными математическими методами, которые используются как в защите информации, так и в технологиях искусственного интеллекта. Упор делается на методы дискретной математики (графы, теория кодирования, комбинаторика, булевы функции), на аппарат математической логики, линейной алгебры, теории игр, теории вероятностей и математической статистики. По желанию слушатели смогут познакомиться с элементами неархимедова анализа и применения его в защите информации.

Вторая важная составляющая магистерской программы – это современные информационные технологии. В первую очередь технологии искусственного интеллекта. Слушатели овладеют основными метода интеллектуального анализа данных, который применяется в

информационных системах. Познакомятся с его недостатками и возможными векторами атак на такие системы.

Уникальность магистерской программы состоит в том, что она находится на стыке теории и практики. Магистры во время обучения не только получают теоретические знания, но и важные практические умения. Значительная часть магистерской программы посвящена практики в области кибербезопасности, устойчивости систем искусственного интеллекта, а также в области разработки систем с применением технологии искусственного интеллекта.

Программа разработана с учётом международного опыта, с привлечением ведущих специалистов в области кибербезопасности и безопасности систем искусственного интеллекта: ОАО «Инфотекс», ООО «Крипто-Про», АО «НПК “Криптонит”», ПАО «Сбер» и др. Разработчики программы – ведущие специалисты в области кибербезопасности, устойчивости систем искусственного интеллекта и защиты информации, в большинстве своём кандидаты и доктора физико-математических наук.

Цели и задачи магистерской программы

Цель: подготовка профессионально компетентных математиков и программистов для решения задач, связанных с безопасностью, робастностью и надежностью систем, построенных с использованием методов искусственного интеллекта и машинного обучения, способных к самостоятельному и творческому ведению деятельности в области разработки с использованием систем искусственного интеллекта устойчивых и безопасных информационных системы, методической и научно-исследовательской деятельности по широкому спектру проблем, связанных с использованием и разработкой устойчивых систем искусственного интеллекта на различных образовательных ступенях и в различных образовательных и научных организациях.

Задачи:

- овладение современной методологией и технологией разработки информационных систем с использованием технологии искусственного интеллекта;
- овладение современной методологией и технологией разработки систем обеспечения кибербезопасности;
- овладение современной методологией и технологией обеспечения робастности систем искусственного интеллекта;
- подготовка высококвалифицированного специалиста, готового к осуществлению инновационной профессиональной деятельности в области кибербезопасности и искусственного интеллекта.

Предусмотрено прохождение научно-исследовательской и технологической практик.

Области профессиональной деятельности выпускника

Магистерская программа направлена на углубление и расширение базовых знаний, полученных слушателем на предыдущих ступенях системы государственного образования, овладение современной методологией и технологией построения информационных систем, использующих технологии искусственного интеллекта с учётом требований кибербезопасности, а также построения систем кибербезопасности на базе технологии интеллектуального анализа данных.

Выпускник магистерской программы получает базовое профильное образование, делающее его востребованным специалистом в различных организациях, которые создают и/или используют информационные системы на базе технологий искусственного интеллекта, в образовательных и научно-исследовательских организациях различного типа для проведения исследований в области кибербезопасности и робастности систем искусственного интеллекта.

Выпускник, успешно освоивший программу, будет обладать:

общекультурными компетенциями (готов использовать знания современных проблем науки и образования при решении задач кибербезопасности и безопасности искусственного интеллекта),

общепрофессиональными компетенциями (способен применять современные методики и технологии в задачах обеспечения кибербезопасности и безопасности искусственного интеллекта; способен анализировать результаты научных исследований и применять их при решении конкретных задач в области обеспечения кибербезопасности и безопасности искусственного интеллекта)

профессионально-специализированными компетенциями (готов к использованию методологии и методов научного исследования в области обеспечения кибербезопасности и безопасности искусственного интеллекта).

Трудоустройство: выпускники могут работать в коммерческих и государственных компаниях, в первую очередь, которые либо используют системы, созданные с применением технологий искусственного интеллекта, либо, которые разрабатывают такие системы, научно-исследовательских организациях различного типа.

Авторы:
академик, д.т.н. Соколов Игорь Анатольевич
доцент, к.ф.-м.н. Чижов Иван Владимирович
доцент, к.ф.-м.н. Гамаюнов Денис Юрьевич
ассистент, Ильюшин Евгений Альбинович