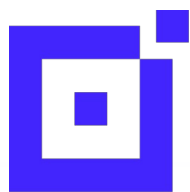


Кросс-отраслевой образовательный центр искусственного интеллекта

Санкт-Петербургский политехнический университет Петра Великого

Супрун Александр Федорович, доцент, к.т.н.,
Высшая Школа Кибербезопасности СПб ПУ

Москва - 2026 г.



Конкурсный отбор вузов

 минцифры_

Лента Министерство Деятельность Документы

[← Вернуться назад](#)

Главная · Лента

29 апреля [Новость Минцифры](#) [# ИТ-образование](#) [# Топ ИИ](#)

Более 20 российских вузов будут готовить топ-специалистов в сфере ИИ к 2030 году

Москва, 29 апреля 2025 года — Завершён конкурсный отбор вузов, которые с 2025 по 2030 годы будут готовить высококвалифицированных специалистов в области искусственного интеллекта. Победители получат поддержку в рамках федпроекта «Искусственный интеллект» нацпроекта «Экономика данных и цифровая трансформация государства».

Как проходил отбор

Вузы отбирались по двум уровням — ДС («Data Science») и ТОП ДС («Top Data Science»). Специалисты уровня ТОП ДС смогут принимать участие в научных исследованиях в области ИИ или самостоятельно их проводить, создавать новые методы обучения ИИ, проектировать архитектуру моделей ИИ мирового уровня. Специалисты уровня ДС — заниматься настройкой и дообучением существующих моделей ИИ, а также решением прикладных задач.

Вузы, которые прошли отбор на уровень ТОП ДС

- Национальный исследовательский университет «Высшая школа экономики»
- Национальный исследовательский университет ИТМО
- Университет Иннополис
- Московский физико-технический институт (национальный исследовательский университет)
- Санкт-Петербургский государственный университет
- Южный федеральный университет

Вузы, которые прошли отбор на уровень ДС

- Национальный исследовательский университет ИТМО
- Университет Иннополис
- Южный федеральный университет
- Новосибирский национальный исследовательский государственный университет
- Московский технический университет связи и информатики
- Финансовый университет при Правительстве РФ
- Российский университет дружбы народов имени Патриса Лумумбы
- Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
- Национальный исследовательский ядерный университет «МИФИ»
- Российский экономический университет имени Г.В. Плеханова
- Санкт-Петербургский политехнический университет Петра Великого
- Южно-Уральский государственный университет
- Волгоградский государственный технический университет
- Поволжский государственный технологический университет
- Российский государственный аграрный университет – МСХА имени К.А. Тимирязева
- Кубанский государственный университет
- Вятский государственный университет
- Севастопольский государственный университет
- Рязанский государственный радиотехнический университет имени В.Ф. Уткина



Образовательные программы топ-уровня

Название программы	Направление подготовки	Проф. роли	Образ выпускника	Индустриальные партнеры
Технологии машинного обучения и искусственного интеллекта	02.03.01 «Математика и компьютерные науки»	 ML Engineer  AI Architect	- пишет качественный код на python, java, C/C++ и других языках программирования - работает с суперкомпьютерами и современными облачными системами - владеет прикладными инструментами в области машинного обучения	
Технологии интеллектуального анализа данных	02.03.03 «Математическое обеспечение и администрирование информационных систем»	 Data Engineer  Data Architect	- создает реляционную и нереляционную базу данных, а также осуществляет ее поддержку и администрирование - пишет качественный код на python, java, C/C++ - работает с современными облачными системами и средствами виртуализации, а также с прикладными инструментами в области машинного обучения и больших данных	
Безопасность компьютерных систем (Технологии искусственного интеллекта в кибербезопасности)	10.03.01 «Информационная безопасность»	 ML Engineer (in cybersecurity)  AI Security Engineer	- решает прикладные задачи в области обеспечения безопасности компьютерных систем и объектов различного уровня в условиях существования угроз в информационной сфере с применением технологий искусственного интеллекта - обеспечивает устойчивость систем искусственного интеллекта к деструктивным воздействиям	  ВКОНТАКТЕ Нильсен



Реализация 1-ого года образовательных программ на практике

Гостевые лекции

от экспертов из «РТК ИТ», «ВКонтакте», «Сбер» и «Позитив Текнолоджиз»

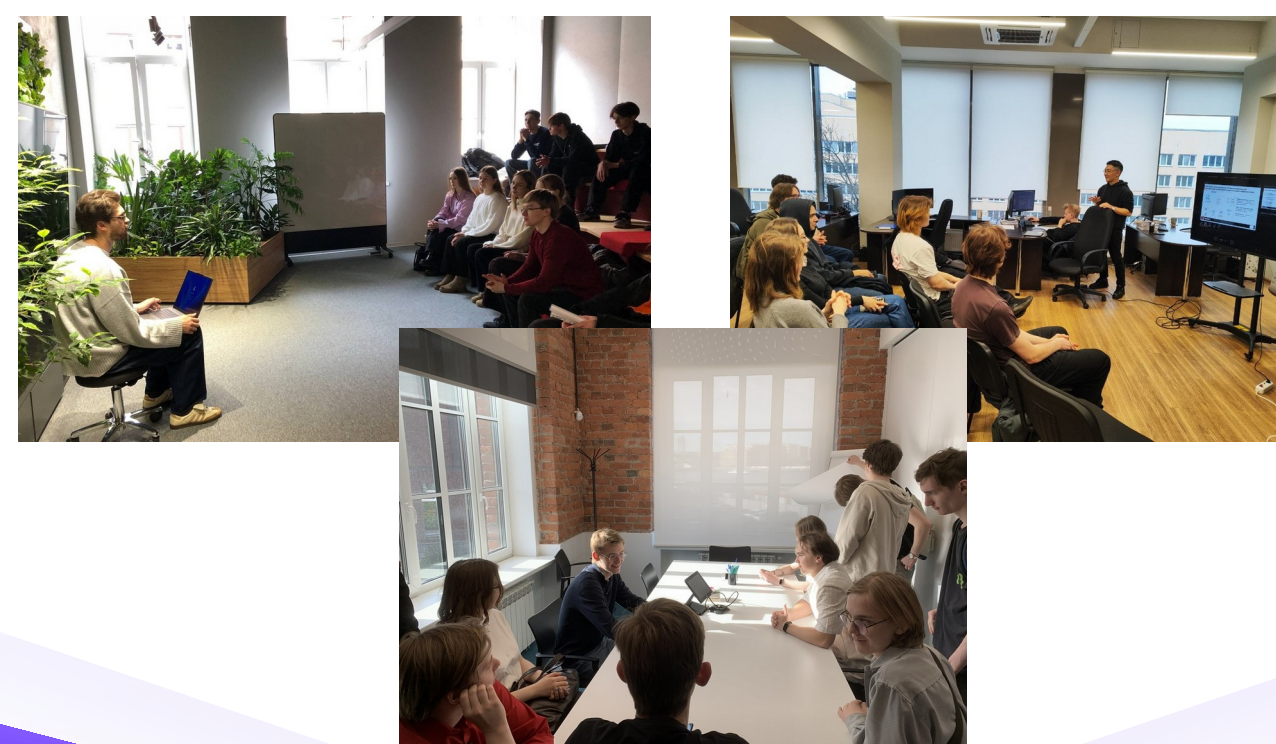


Расширение стандартной академической программы

- уникальный практический опыт и знания от экспертов из индустрии
- живое общение с экспертом-ориентиром
- понимание реальных перспектив своей будущей карьеры

Практика в ИТ-компаниях

практика и посещение офисов «Необит», «Позитив Текнолоджиз» и «Сбер»



Выполнение проектов, основанных на реальных бизнес-кейсах

- прототип харнеса под ИИ-агента для тулинга SAST/DAST
- проект по развертыванию и настройке SIEM-системы на базе ИИ
- аналитическое исследование уязвимостей в системах на базе ИИ

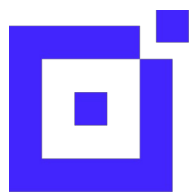
Хакатоны и деловые игры

«Чемпионат по ИИ» (РТК ИТ), «НеоКвест», «Деловая игра» (СПБПУ)



Вход в комьюнити и командная работа

- прототип RAG-системы (векторный поиск по коду с веб-интерфейсом)
- проект по исследованию семантического поиска в коде
- получение навыков командной работы (по методике Белибна)



Реализация 1-ого года образовательных программ на практике

Прототип харнеса под ИИ-агента для тулинга SAST/DAST

Практика в ООО «Необит»
Команда из 5 первокурсников 10.03.01

Результаты:

1. Настроен исследовательский стенд.
2. Выполнен анализ функционала ПО.
3. Проведено сканирование улов стендов.
4. Выполнен поиск существующих исследований по анализу защищенности ПО.
5. Выполнен анализ актуальных векторов воздействия, сетевой и локальной поверхности атаки, а также компонентов ПО.
6. Выполнен анализ безопасности ПО методами статического и динамического анализа.
7. Исследована возможность автоматизации анализа с помощью LLM-агентов, интегрированных с SAST- и DAST-инструментами. Выполнена интеграция LLM-агента с двумя инструментами.



Развертывание и настройка SIEM-системы на базе ИИ

Практика в АО «Позитив Текнолоджиз»
Команда из 3 первокурсников 10.03.01

Результаты:

1. Развернута SIEM-система Wazuh
 - Установлен сервер Wazuh.
2. Настроена Wazuh
 - Сконфигурированы правила, шаблоны индексов и интеграцию с визуализатором.
3. Подключен агент
 - Установлена и зарегистрирована клиентская машина-агент.
 - Проверено, что события (логи) успешно поступают в сервер Wazuh.
 - Добавлены базовые фильтры
 - Создано несколько простых фильтров (по типу источника, уровню угроз, конкретным событиям).
 - Продемонстрировано, как пользоваться фильтрацией на базовом уровне.

В результате выполнения работы была успешно развёрнута система SIEM Wazuh на сервере Debian 12, подключен клиентский агент Windows 10, настроены правила фильтрации и активирована система мониторинга. За время тестирования система обработала более 150 событий безопасности, успешно идентифицировав 3 подозрительных процесса и 2 попытки несанкционированного доступа...

Прототип RAG-системы (векторный поиск по коду с веб-интерфейсом)

Участие в «Чемпионате по ИИ»
Команда из 4 первокурсников 02.03.01

Результаты:

Семантический поиск по Python-коду: парсинг через ast → обогащение в NL-текст → эмбединги → векторный поиск с опциональными каналами (BM25/RRF, HyDE, multi-query, MMR, cross-encoder). Сверху - чат с history-aware RAG и админка кодовой базы.

Один код и одни образы на два профиля: small (одна нода, без k8s) и large (кластер на k8s/Helm/Argo CD). Профили отличаются только реализациями за интерфейсами (Chroma ↔ Qdrant, SQLite ↔ Postgres, in-process ↔ Redis) и масштабом, не логикой.

Подробнее с проектом можно ознакомиться по ссылке: <https://github.com/drysl0/CodeLens>

Слои (снизу вверх)

1. domain - models.py (структура Chunk) и interfaces.py (абстрактные порты). Ни от чего не зависит, от него зависит всё.
2. adapters - реализации портов: парсеры (indexing/parsers), эмбедедер (embeddings), перанкер (reranking), вектор-стор (stores), релеяонка (persistence), LLM (llm).
3. orchestration - retrieval/hybrid.py (HybridRetriever - оркестратор поиска: dense/bm25/hyde/rerank/mmr + cache-aside поверх чистого ядра), clients/backend.py (LocalBackend - чат, ответы, админка; кэш реестра/ответов и инвалидация поиска).
4. composition root - factory.py собирает всё по конфигу.
5. endpoints - index.py (CLI), app.py (UI), evaluate.py (метрика), services/* (REST).

Правило зависимостей: внешние слои зависят от внутренних, не наоборот. Любая реализация подключается через интерфейс из domain/interfaces.py.



Ключевые изменения в образовательных программах

Что изменено

- Целевая компетентностная модель выпускника (ЦКМВ) приведена в соответствие с утвержденной КРМ и согласована с индустриальным партнером
- Расширен состав Центра
- К проведению занятий привлекается больше специалистов-практиков
- Индустриальный партнер предоставил доступ для обучающихся и преподавателей к сервисам и вычислительным мощностям
- Темы ВКР согласуются с индустриальным партнером
- Представители индустриальных партнеров присутствуют на защитах ВКР

Основной результат актуализации: образовательные программы соответствуют установленным требованиям к программам уровня ТОП-ИИ

Как это повлияло на реализацию программы

- В дисциплины добавлены разделы, посвященные практическому применению технологий МО и ИИ
- Преподаватели сфокусированы на реализации дисциплин в рамках ООП топ-уровня
- С 1 курса студенты выполняют проекты, основанные на реальных бизнес-кейсах, под руководством наставников из индустрии
- Расширение ресурсной базы позволило обновить содержание дисциплин, связанных с применением больших языковых моделей
- Темы ВКР будут базироваться на реальных бизнес-кейсах
- Более объективная оценка ВКР

Основной результат актуализации: студенты получают именно те компетенции, которые востребованы у работодателей

Ключевые результаты:

1

Что сработало

Практико-ориентированные
иммерсивные
образовательные подходы

2

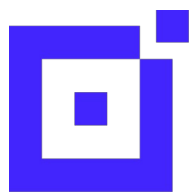
Что получили студенты

Погружение в реальные кейсы
и специфику отрасли,
знакомство с корпоративной
культурой

3

Что дала работа с индустрией

Реальные бизнес-кейсы,
экспертная поддержка
менторов, подтверждение
компетенций



Участие индустриального партнера в реализации образовательной программы



Вклад компании в реализацию программы

Постановка задач

- векторный поиск по коду с веб-интерфейсом
- исследование семантического поиска в коде

Наставничество

- вебинары
- мессенджеры
- электронная почта

Ресурсы и инфраструктура

- доступ к сервису «Нейрошлюз»
- предоставление доступа к облачным вычислительным ресурсам

Экспертиза

- проведение вебинаров в рамках Чемпионата по ИИ
- оценка презентаций по проектам

Что показали студенты

Результаты (примеры):

- разработан Умный поиск по кодовой базе (CodeLens), состоящий из 4 основных модулей: модуль парсинга и векторизации, гибридная поисковая система (ChromaDB + BM25), веб-интерфейс (Streamlit) и аналитический LLM-модуль (<https://github.com/Eugeniouo/CodeLens>)
- разработан прототип RAG-системы для автоматического анализа, индексирования и семантического поиска по Python-кодовой базе, состоящий из AST-парсер и Chunker, векторной базы данных, модели эмбедингов и веб-интерфейса с гибридным поиском (<https://github.com/UserName1212/RAG-System>)

Сильные стороны студентов: быстрая обучаемость, высокий уровень фундаментальной подготовки и инженерной культуры, умение работать в команде

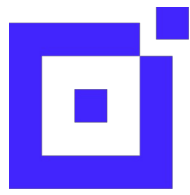
Компетенции на достаточном уровне: умение писать качественный код, понимание алгоритмов и структур данных, умение работать с ИИ-библиотеками, использование систем контроля версий и сред разработки, понимание работы ОС

Планы дальнейшего сотрудничества (на 2026 г.)

- Привлечение сотрудников ООО «РТК ИТ» для преподавания отдельных дисциплин
- Организация практик студентов на базе ООО «РТК ИТ»
- Экспертиза и актуализация РПД специалистами ООО «РТК ИТ»
- Усиление компетенций студентов: технические навыки в области ИТ и ИИ, креативное мышление, навыки командной работы и проектного менеджмента

Команда СПбПУ заняла первое место на Чемпионате по ИИ





Ответы на вопросы

1. Чем программа отличается от классических ИТ- и кибербезопасностных направлений?

Программа направлена на подготовку специалистов, способных решать прикладные задачи в области кибербезопасности, в том числе за счет применения технологий ИИ. Отличительной особенностью является интеграция в учебный план разделов, связанных с использованием методов машинного обучения, нейросетевых моделей и биоинспирированных алгоритмов. Также в реализации программы активное участие принимают специалисты-практики, что позволяет расширить стандартную академическую программу, предоставляя студентам возможность получить уникальный практический опыт и знания от экспертов из индустрии.

2. Какие ключевые навыки и технологии изучают студенты?

Учебный план предполагает классическую ИБ-подготовку (безопасность сетей и ОС, криптография), которая сочетается с относительно новыми учебными дисциплинами, такими как реверс-инжиниринг, многоагентные системы, объяснимость и доверие к ИИ. По окончании обучения наши выпускники будут способны заниматься настройкой и дообучением моделей ИИ и МО для защиты объектов информатизации, а также обеспечением устойчивости систем ИИ к деструктивным воздействиям.

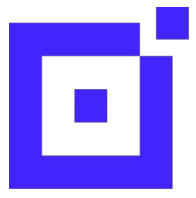
3. Как в обучении применяется искусственный интеллект?

В первую очередь ИИ является объектом изучения. С первого курса у студентов формируется понимание, для решения каких задач в области кибербезопасности следует применять те или иные методы ИИ, а где лучше подойдут традиционные проверенные временем решения. Наличие высокопроизводительного оборудования и доступа к платформам нашего «якорного» индустриального партнера ООО «РТК ИТ» позволяет студентам как разворачивать свои нейросетевые модели с нуля, так и использовать готовые коммерческие решения в ходе выполнения лабораторных и курсовых работ.



Легче переносить терпеливо то, что нам не дано исправить.
Квинт Гораций Флакк

Спасибо за внимание



Контакты Центра

<https://top-ai.spbstu.ru/>

Адрес:

195 251, Санкт-Петербург, Политехническая, ул., д. 29, 3-й учебный корпус, каб. 308

Для связи:

+7 (812) 297-16-28 - для организаций

+7 (812) 297-16-47 - для студентов

iccs@spbstu.ru - для организаций

iccs_office@spbstu.ru - для студентов