

# доверенный искусственный интеллект

# магистратура



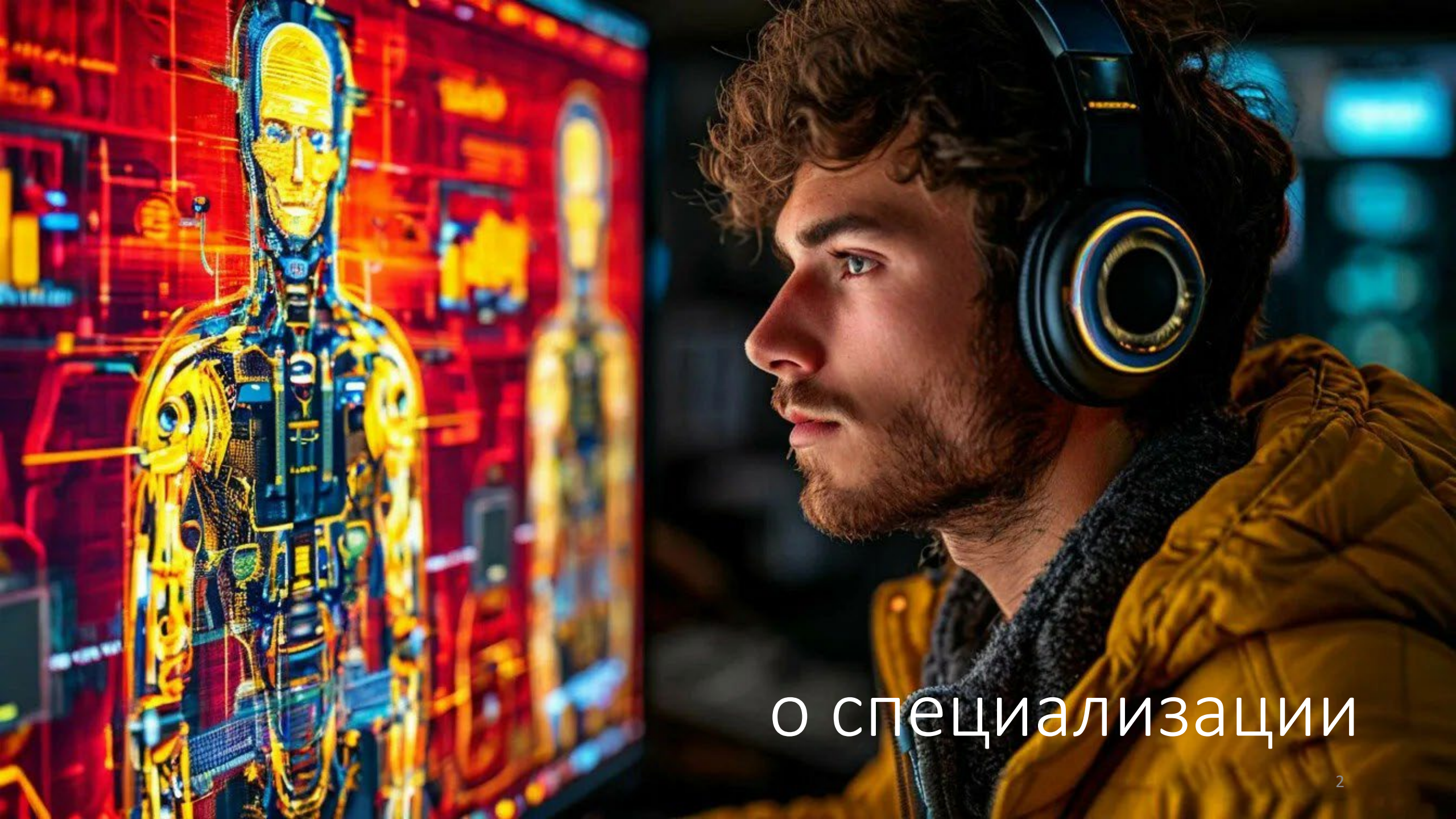
ФРКТ

кафедра  
защиты  
информации

ОКБ САПР

Специализация  
03.04.01  
«Прикладная  
математика  
и физика»





о специализации

# ВАШЕ ВРЕМЯ ДЛЯ ДОСТИЖЕНИЙ МИРОВОГО УРОВНЯ



Базовая организация кафедры защиты информации ФРКТ МФТИ – ОКБ САПР – разработчики средств защиты информации.

Мы занимаемся этим более 35 лет, и очень многое сделали первыми в Мире.

Мы знаем, насколько это не только приятно, то и важно.

Сейчас на пике научно-технической мысли – системы искусственного интеллекта.

Поэтому именно их мы предлагаем в качестве объекта деятельности нашим магистрантам.

Здесь есть что сделать первыми в Мире.  
А мы поможем.



# ДОВЕРЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Специализация объединяет 2 глобальные задачи, каждая из которых – это целое направление исследований.

1. Как сделать системы искусственного интеллекта (ИИ) доверенными.
2. Как использовать системы ИИ для обеспечения защиты информации.

Обе задачи абсолютно новые, находятся на стадии формирования задач и формулирования начальных гипотез.




# КАК СДЕЛАТЬ СИСТЕМЫ ИИ ДОВЕРЕННЫМИ

Объект изучения в этом направлении исследований – именно **системы ИИ**, а не алгоритмы, не технологии, не ИИ сам по себе как феномен или философское понятие.

**Доверенные системы ИИ** – то есть такие, которым можно доверять, контролируемые.

На текущем уровне развития науки и техники – это комплекс научных задач с перспективами инженерных решений.



# КАК СИСТЕМЫ ИИ МОГУТ ИСПОЛЬЗОВАТЬСЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

В этой области задач открываются такие заманчивые перспективы, что многократно возрастает опасность шарлатанства (по злому умыслу или наивности).

Определить место систем ИИ **в технологиях защиты информации** и создать эффективные решения на их основе – задача этого направления специализации.

Пример, который позволит представить себе это направление наглядно – **интерактивная биометрическая идентификация человека** на основе рефлекторной дуги – например, по траектории слежения взглядом за произвольным стимулом.

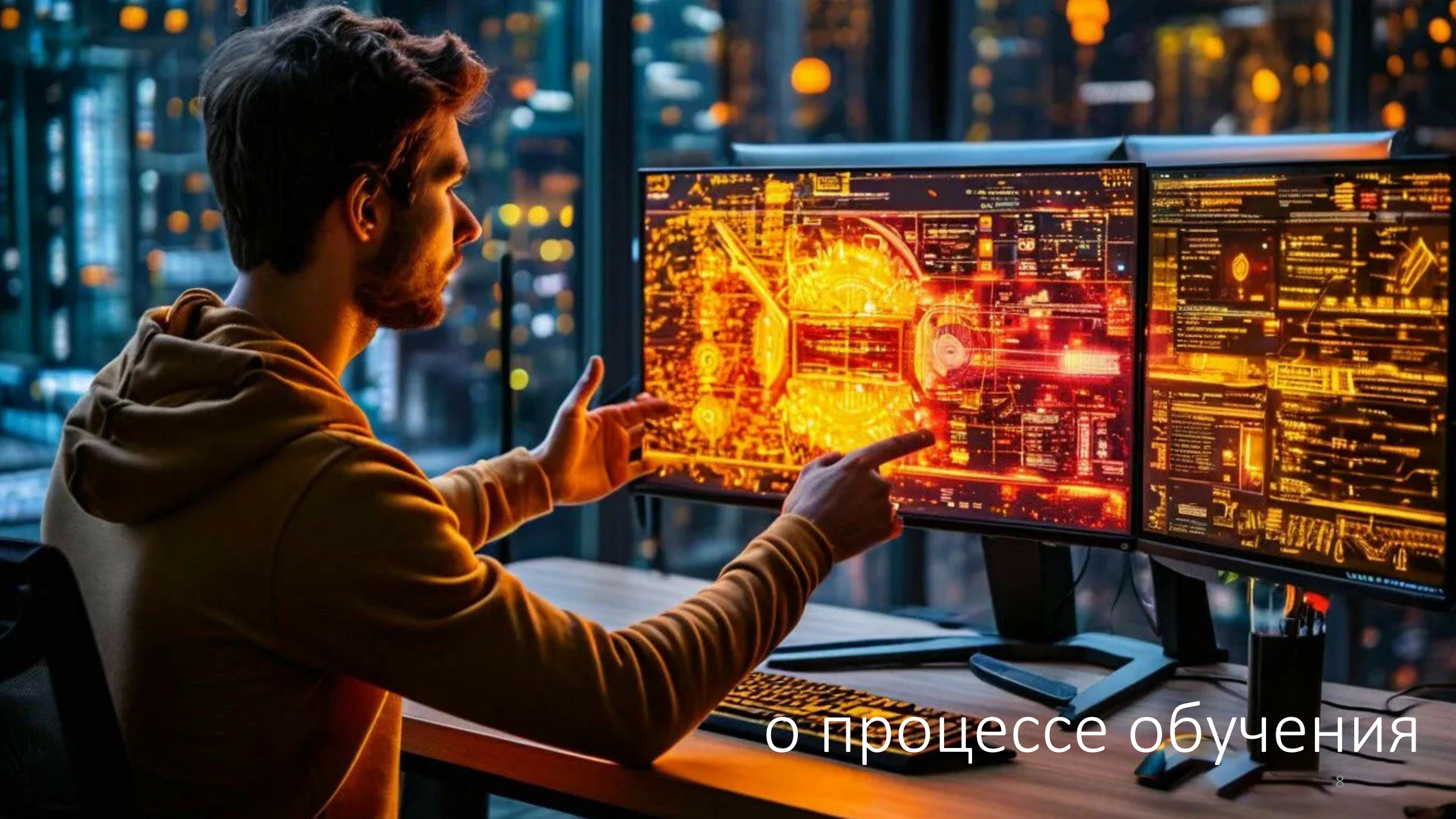


# ПРЕПОДАВАТЕЛИ БАЗОВЫХ ДИСЦИПЛИН

Все базовые дисциплины магистратуры «Доверенный искусственный интеллект» ведут

- преподаватели **кафедры** защиты информации ФРКТ МФТИ;
- сотрудники **ОКБ САПР**, непосредственно занимающиеся разработкой средств защиты информации;
- сотрудники **РЕД СОФТ**, непосредственно занимающиеся разработкой отечественных операционных систем.

Именно они также руководят научно-исследовательскими работами магистрантов и курируют их практические задачи.



о процессе обучения



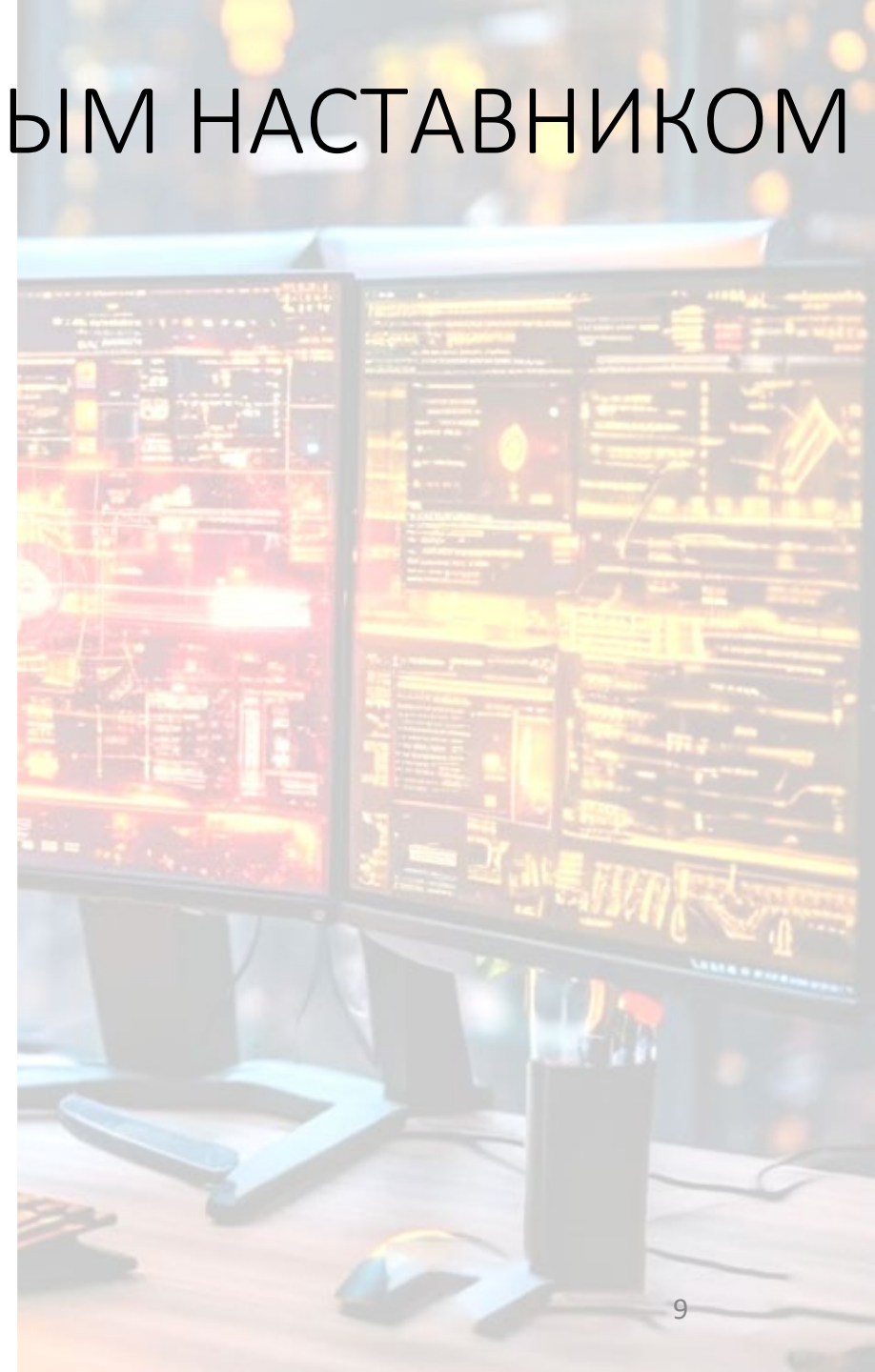
# ОБУЧЕНИЕ ЧЕРЕЗ ПРАКТИКУ С ЛИЧНЫМ НАСТАВНИКОМ

Обучение в магистратуре ощутимо ориентировано на практику:

соотношение теоретических и практических занятий 20/80 (в пользу практики).

На практике магистранты приобретут умения и выработают навыки по

- проектированию систем;
- интеграции;
- планированию, проведению и оценке результатов экспериментов;
- математическому моделированию;
- инженерной (физической) защите.



# СПИСОК ДИСЦИПЛИН МАГИСТРАТУРЫ

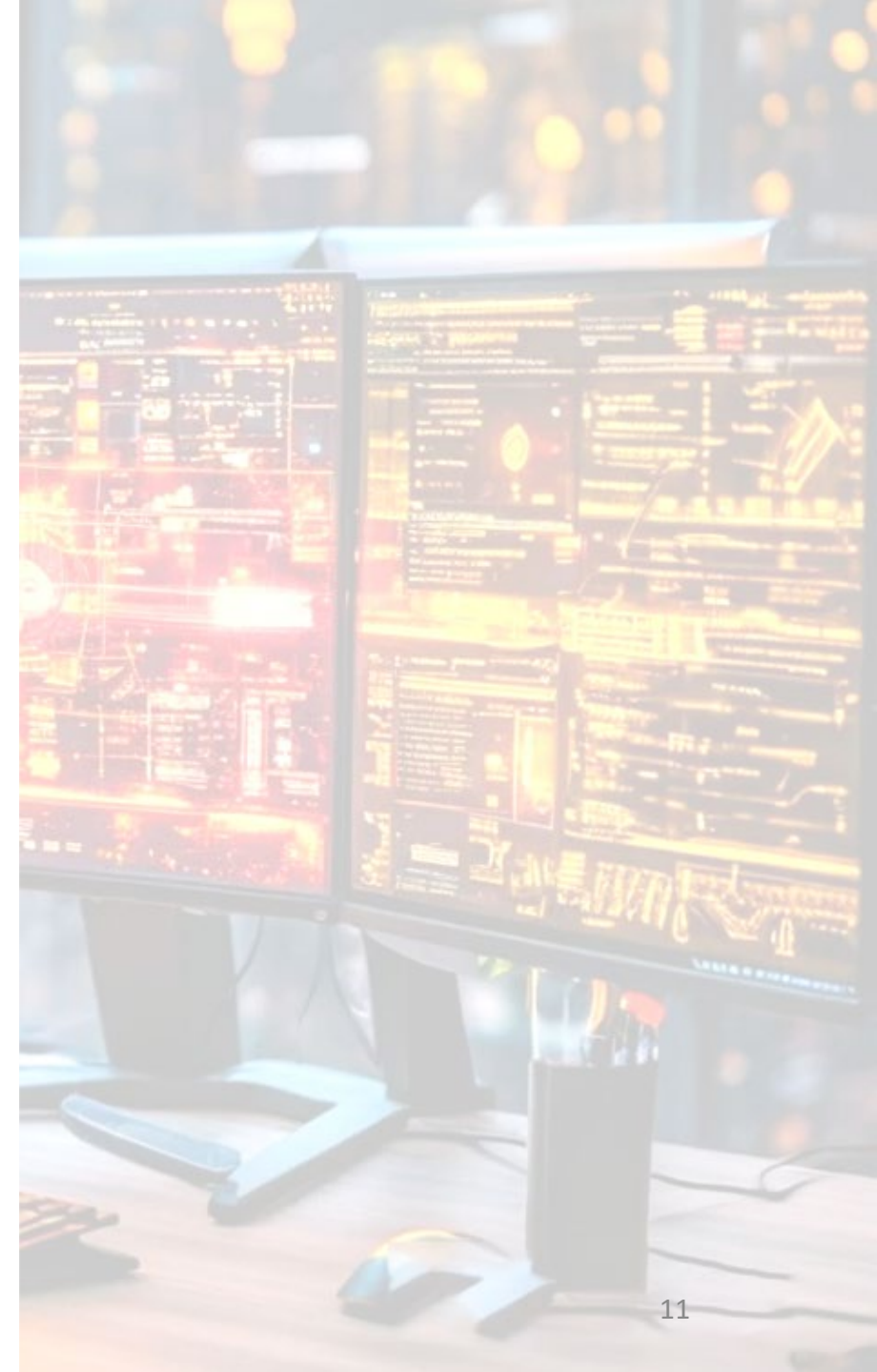
- Основы информационной безопасности – 9 семестр, ОКБ САПР
- Обеспечение качества доверенных систем – 9 семестр, ОКБ САПР
- Средства обеспечения безопасности доверенных систем – 9 семестр, ОКБ САПР
- Правовое регулирование информационной безопасности – 9 и 10 семестр, ОКБ САПР
- Основы научного исследования – 9 и 10 семестр, ОКБ САПР
- Технологии создания доверенных информационных систем – 10 семестр, ОКБ САПР
- Операционные системы и доверенные платформы – 10 и 11 семестр, РЕД СОФТ
- Организация инфраструктуры открытых ключей в доверенных системах – 10 и 11 семестр, ОКБ САПР
- Иностранные языки (язык по выбору) – 9 и 10 семестр, МФТИ
- Гуманитарный и социальный цикл (модуль по выбору) – 9 и 10 семестр, МФТИ

**В 11 семестре занятия проводятся факультативно.**

# МЕСТО И ВРЕМЯ ЗАНЯТИЙ

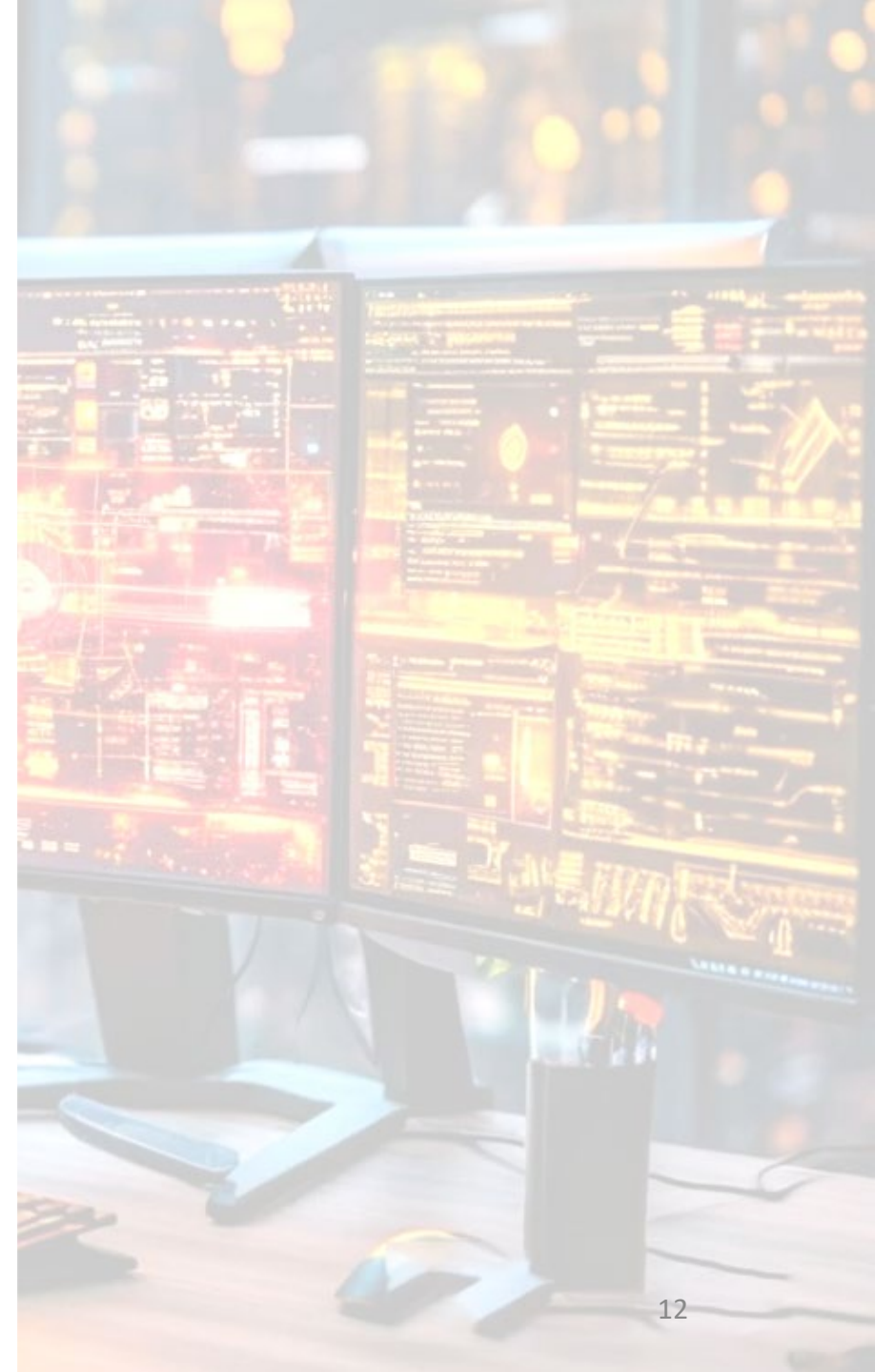
Гуманитарный цикл и иностранные языки проходят в Долгопрудном, в общем потоке МФТИ по понедельникам и субботам.

Базовые дисциплины проходят со вторника по пятницу в ОКБ САПР, в Москве, на Павелецкой.



# ПОЛЕЗНЫЕ СВЕДЕНИЯ

- **Стипендия** выплачивается на всем протяжении обучения.
- Работа в базовой организации в период обучения – **дополнительно оплачивается** и обязательно связана с учебными дисциплинами.
- Работу по каждой задаче **курирует наставник**.
- Возможно **отчисление** за низкие учебные результаты, в том числе – за неудовлетворительные результаты НИР.



# ОБЩЕЖИТИЕ

The screenshot shows a routing application interface with a green header. The start point is 'Московский физико-технический' (A) and the end point is 'ОКБ САПР, Производственная кс' (B). Below the header are icons for filters and transport modes. Three route options are listed:

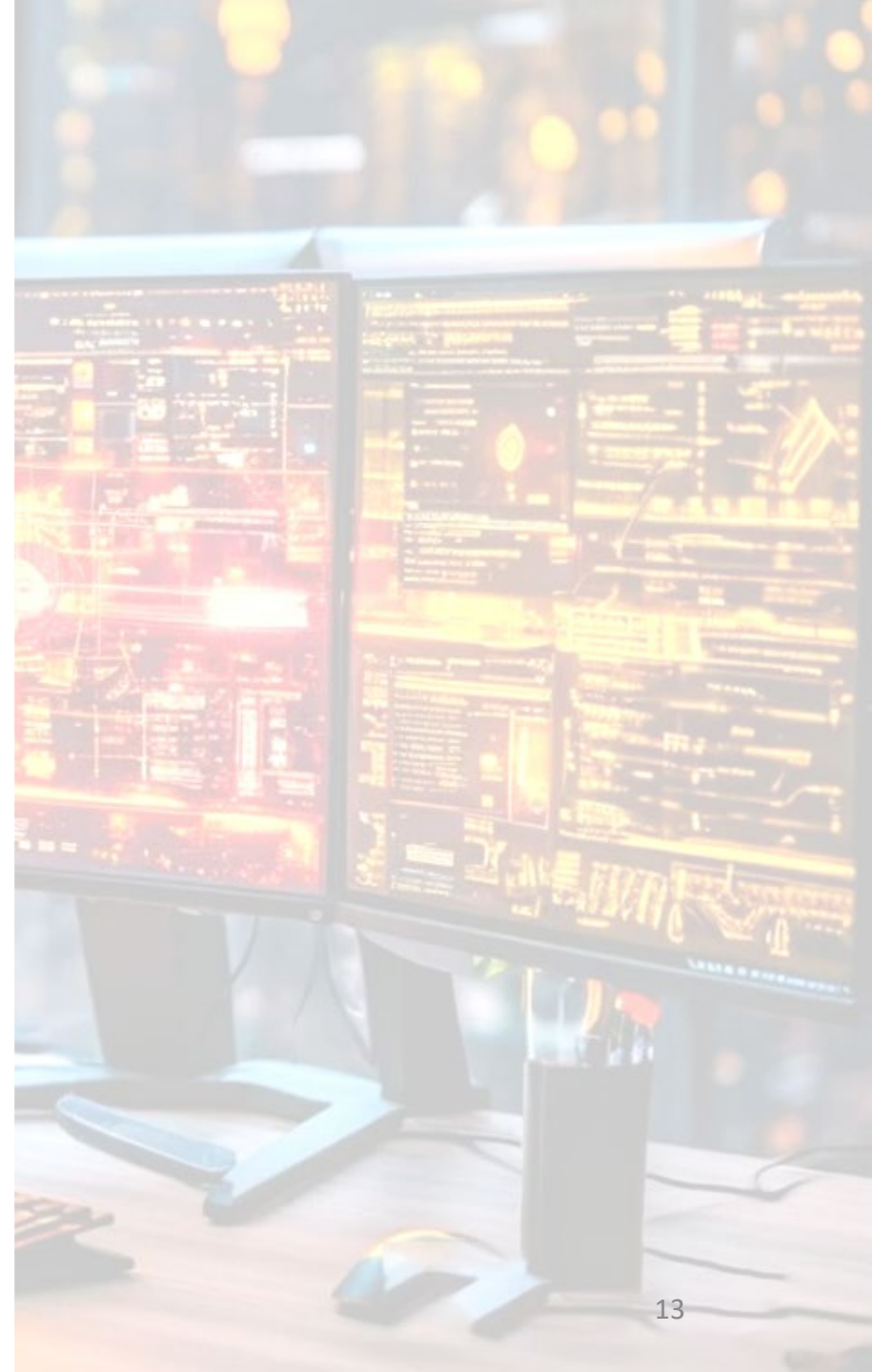
- 52 мин** (1 пересадка): Пешком 28 мин. The route consists of walking (10 мин), Metro Line 11 (11), Metro Line 2 (2), and walking (18 мин).
- 55 мин** (2 пересадки): Пешком 30 мин. The route consists of walking (1 мин), Bus (+2), Metro Line 9 (9), Metro Line 5 (5), and walking (22 мин).
- 1 час** (без пересадок): Пешком 45 мин. The route consists of walking (15 мин), Metro Line 9 (9), and walking (29 мин).

At the bottom, there is a button: [Отправить маршрут на телефон](#)

Общежитие предоставляется в Москве, в районе метро Зюзино и Каховская.

Это удобнее, чем в Долгопрудном, поскольку именно в Москве проходит большая часть занятий.

Дорога от общежития до места проведения занятий (Павелецкая, ОКБ САПР) занимает меньше часа.





О ПОСТУПЛЕНИИ



# МАГИСТРАНТУ ПОНАДОБЯТСЯ

знания и умения по

- радиоэлектронике,
- программированию,
- конструированию.



# ЖЕЛАТЕЛЬНЫЕ СКЛОННОСТИ

Обучение в магистратуре «Доверенный искусственный интеллект» будет приятнее тем, кто

- обладает конкретным мышлением и
- кому нравится работать с материальными объектами – оборудованием, приборами, элементной базой и экспериментальными установками.






# • ДЛ Я ПОСТУПЛЕНИЯ ДОСТАТОЧНО

- иметь законченное образование не ниже бакалавриата,
- сдать стандартные вступительные экзамены магистратуры ФРКТ МФТИ,
- подать заявление-анкету,
- пройти собеседование на специализацию.

**ВНИМАНИЕ!** Порядок этих действий будет одинаковым для бакалавров МФТИ и для поступающих с других стартовых позиций!

# ПРОЦЕСС ПОСТУПЛЕНИЯ

- Подаете заявление в магистратуру здесь:  
<https://pk.mipt.ru> (прием заявлений начинается 10 апреля), указываете в заявлении физтех-школу (ФРКТ) и кафедру (кафедра защиты информации);
- Получаете сообщение (а затем и напоминание), когда ближайший экзамен (это может быть середина мая или, затем, июль);
- Сдаете экзамен;
- Заполняете анкету-заявку на специализацию «Доверенный искусственный интеллект» по ссылке:  
<https://forms.gle/6wiRWtHgBMowEzdr5>
- Мы с Вами свяжемся.

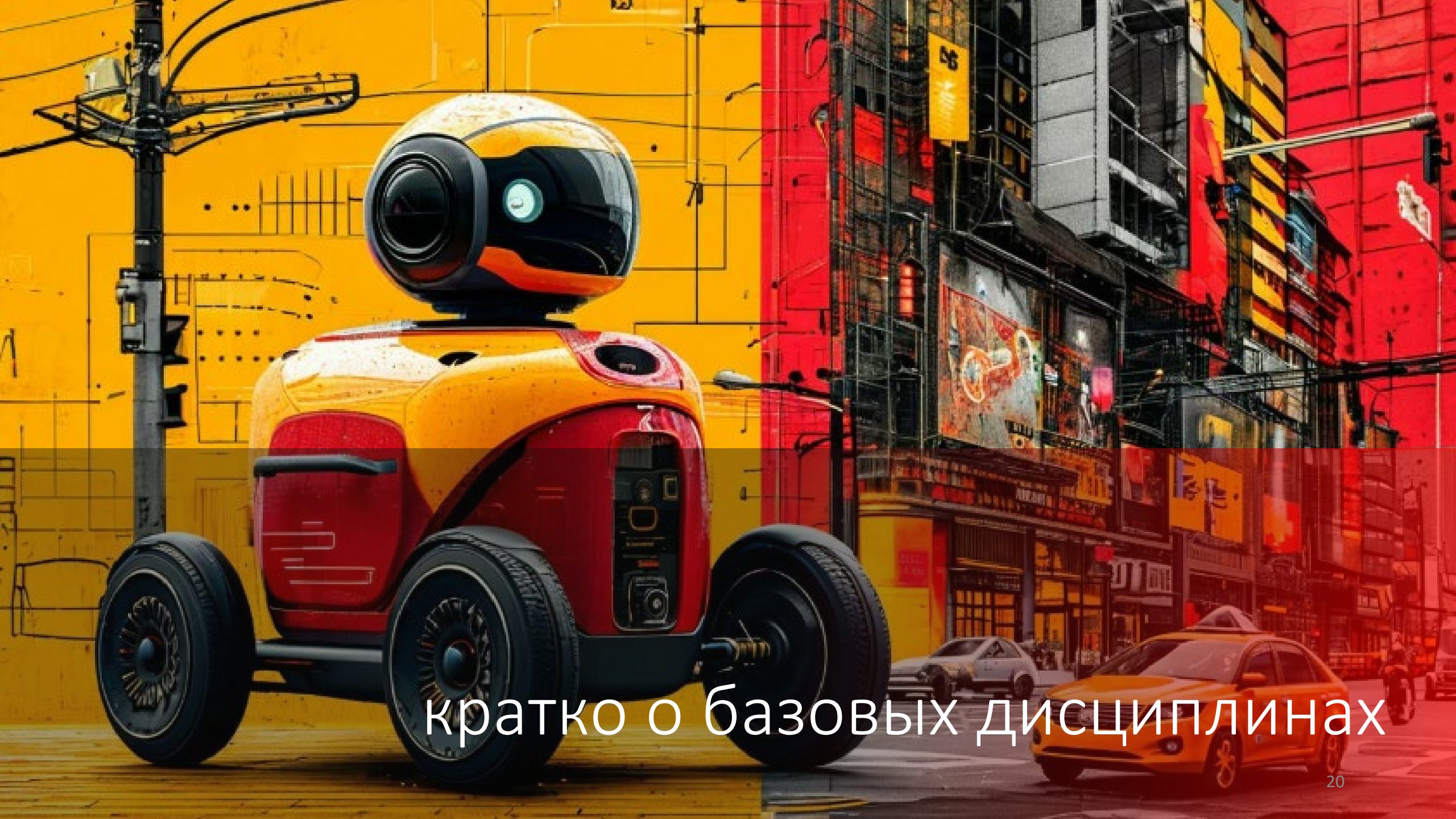


# ИИ ВАС ТОЧНО НЕ ЗАМЕНИТ

Главное, зачем вы идете на эту специализацию?

Чтобы стать **незаменимым** в условиях, когда системы ИИ угрожают профессиональной востребованности все большего круга специалистов.

**ИИ точно не заменит тех, кто умеет делать его доверенным.**



кратко о базовых дисциплинах

# Основы информационной безопасности

Знакомство с наукой защиты информации.

## Узнаем

- основные понятия и основные направления науки;
- основные виды угроз и нарушителей;
- причины уязвимости информационных систем;
- особенности построения информационной структуры в РФ;
- нормативное и правовое регулирование защиты информации в РФ;
- криптографическая защита данных
- модели ИБ.

Для успешного прохождения курса необходимо посещение и конспектирование лекций, самостоятельная работа с дополнительными литературными источниками.

# Обеспечение качества доверенных систем

Знакомство с основами законодательства РФ о доверенных информационных технологиях и обеспечении их качества.

## Узнаем

порядок аттестации объектов информатизации;  
правовые основы лицензирования и сертификации в области защиты информации, в том числе в отношении средств криптографической защиты информации;  
обязательные требования ФСТЭК России и ФСБ России в области защиты конфиденциальной информации;

## Научимся

подготавливать документы, необходимые для проведения процедур лицензирования и сертификации в области защиты конфиденциальной информации, а также аттестации объектов информатизации.

# Средства обеспечения безопасности доверенных систем

Знакомство с современными средствами обеспечения информационной безопасности, применяемыми в доверенных системах.

## Узнаем

- принципы организации доверенной среды
- разграничения доступа в операционных системах (ОС),
- разграничения доступа к элементам управления
- разграничения доступа к ресурсу в зависимости от среды
- средствам обеспечения информационной безопасности, реализующие эти принципы при построении доверенных систем.
- принципы защищенного распространения лицензий на ПО и реализующий их программно-аппаратный комплекс.

## Научимся

самостоятельно устанавливать, администрировать и применять современные средства обеспечения безопасности для создания доверенных систем.

# Правовое регулирование информационной безопасности

Знакомство с основами законодательства РФ о безопасности вообще и информационной безопасности в частности.

## Узнаем

- правовые режимы информации ограниченного доступа;
- правовые основы охраны результатов интеллектуальной деятельности;
- понятие и виды преступлений в сфере компьютерной информации;
- правовые основы обеспечения безопасности критической информационной инфраструктуры;
- порядок аттестации объектов информатизации;
- правовые основы лицензирования и сертификации в области защиты информации, в том числе с использованием средств криптографической защиты информации;
- требования ФСТЭК России и ФСБ России в области защиты информации.

**Научимся** подбирать и применять в профессиональной деятельности необходимые нормативные правовые акты.



# Основы научного исследования

**Узнаем**, какие признаки отличают научное от ненаучного и **научимся** их выявлять в исследовании как процессе и в исследовании как результате (научном тексте).

**Узнаем**, какие существуют виды обоснований, и **научимся** уместно их использовать.

**Узнаем**, чем различаются виды определений и **научимся** их правильно применять, анализировать и оценивать.

**Узнаем**, какие виды ошибок свойственны научным исследованиям, чем они отличаются и зачем это нужно знать, **научимся** находить и исправлять ошибки.

**Узнаем**, приемы научного поиска и библиографического поиска, **научимся** планировать научную работу, выбирать тему, составлять конспект.

**Узнаем**, содержание жанровой специфики научных текстов, их отличия на уровне целей, задач, выводов, композиции, **научимся** составлять историю вопроса, не путать пересказ и анализа, анализ и полемику, применять их уместно.

**Узнаем**, правила проведения эксперимента и наблюдения, **научимся** формулировать гипотезы и планировать эксперименты, и мн. др.

**Научимся** методам самоконтроля при проведении исследования и при оформлении его результатов в виде научного текста.

# Технологии создания доверенных информационных систем

Знакомство с принципами построения и основами создания доверенных информационных систем.

## Узнаем

принципы обеспечения доверия к информационным системам,  
основы законодательства РФ в области обеспечения безопасности  
информационных систем

организационные и технические меры, направленные на обеспечение доверия в  
информационных системах.

Научимся проектировать и разрабатывать архитектуры доверенных  
информационных систем.

# Операционные системы и доверенные платформы

Знакомство с основами установки и настройки операционной системы (ОС) GNU/Linux российского производителя, а также встроенные в нее механизмы защиты.

## Узнаем

- методы защиты информации в современных ОС:
  - управление доступом,
  - идентификация,
  - аутентификация,
  - авторизация и др.
- наложенные средства защиты информации в ОС GNU/Linux.

# Операционные системы и доверенные платформы: дополнительные главы

Факультатив, продолжение курса «Операционные системы и доверенные платформы».

## Научимся

- основам настройки операционной системы (ОС) GNU/Linux российского производителя, а также встроенных в нее механизмов защиты;
- методам защиты информации в современных ОС: аудит и обнаружение вторжений и др.

Обсудим некоторые специфические вопросы, косвенно связанные с обеспечением безопасности операционных систем.

# Организация инфраструктуры открытых ключей в доверенных системах

Знакомство с инженерной, прикладной криптографией.

**Научимся** пониманию условий, при которых математические построения обеспечивают достаточный уровень защищенности информации.

Инфраструктуру открытых ключей рассмотрим в применении к средствам защиты информации, а также через техническую реализацию СКЗИ.

На примере инфраструктуры открытых ключей (ИОК) поймем комплексную связь различных аспектов объективной реальности в контексте информационной безопасности.

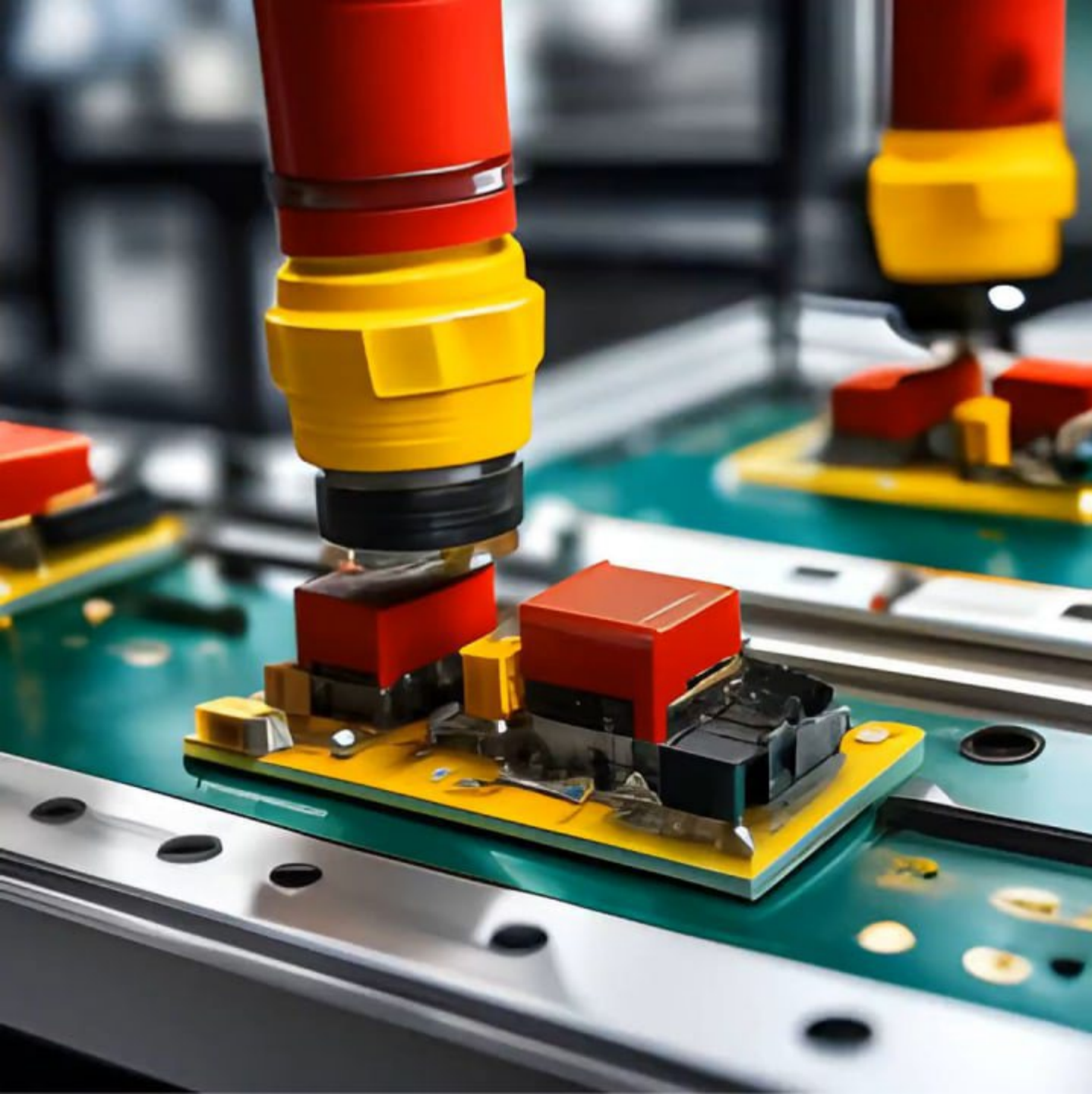
# Организация ИОК в доверенных системах: дополнительные главы

Факультатив, продолжение курса «Организация инфраструктуры открытых ключей в доверенных системах».

В этом продвинутом курсе **узнаем**

- более глубокие аспекты защиты ключевой информации;
- передовые технологии, такие как защита ключей на кристалле и квантовые вычисления.
- принципы защиты от нарушителей высокого класса (что позволяет заглянуть в будущее и коснуться проблем завтрашнего дня).

Курс охватывает темы, находящиеся на переднем крае науки. Он не только знакомит с не самыми популярными аспектами информационной безопасности, но и позволяет лучше осознать всесторонний подход к организации безопасности, а также подвергнуть деконструкции и разумной критике существующие формальные подходы. Этот курс должен показать, что задачи компьютерной и информационной безопасности могут быть не только ремеслом, но и наукой.



# КОНТАКТЫ

Зам. зав. кафедрой  
(магистратура):

Каннер Татьяна Михайловна

[kanner.tm@mipt.ru](mailto:kanner.tm@mipt.ru)

+7-926-235-14-67

заявка тут:

