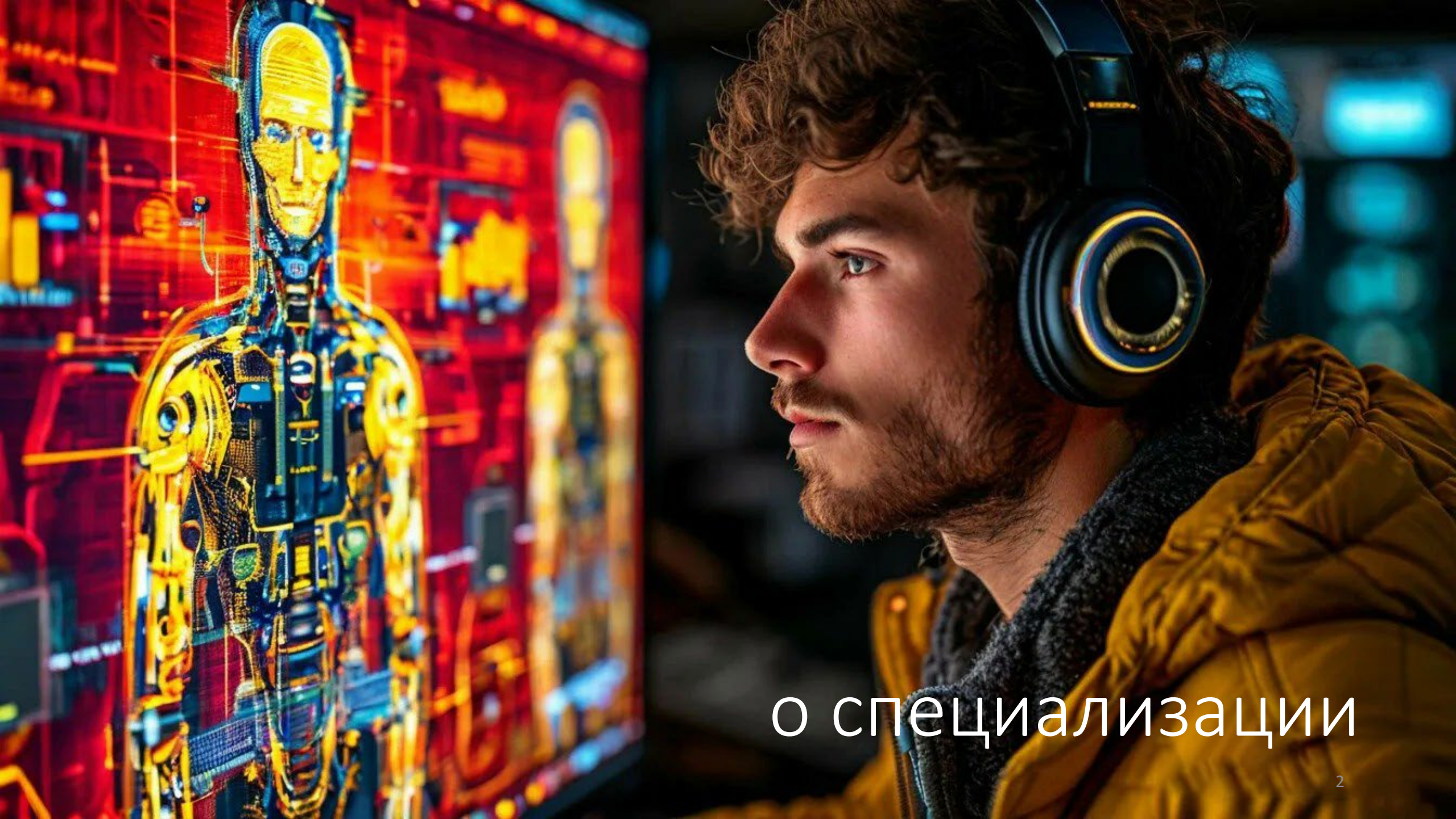
ФРКТ

КАФЕДРА ЗАЩИТЫ ИНФОРМАЦИИ

бакалавриат

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, но и важно.

Постоянно возникающие новые технологии дают огромные возможности и повод для оптимизма. Но не только добропорядочным гражданам, преступникам тоже. Поэтому за появлением каждой новой технологии должна появляться и новая технология защиты.

То есть вам всегда будет что сделать первыми в Мире.
А мы научим, как.

ОСНОВНЫЕ НАПРАВЛЕНИЯ

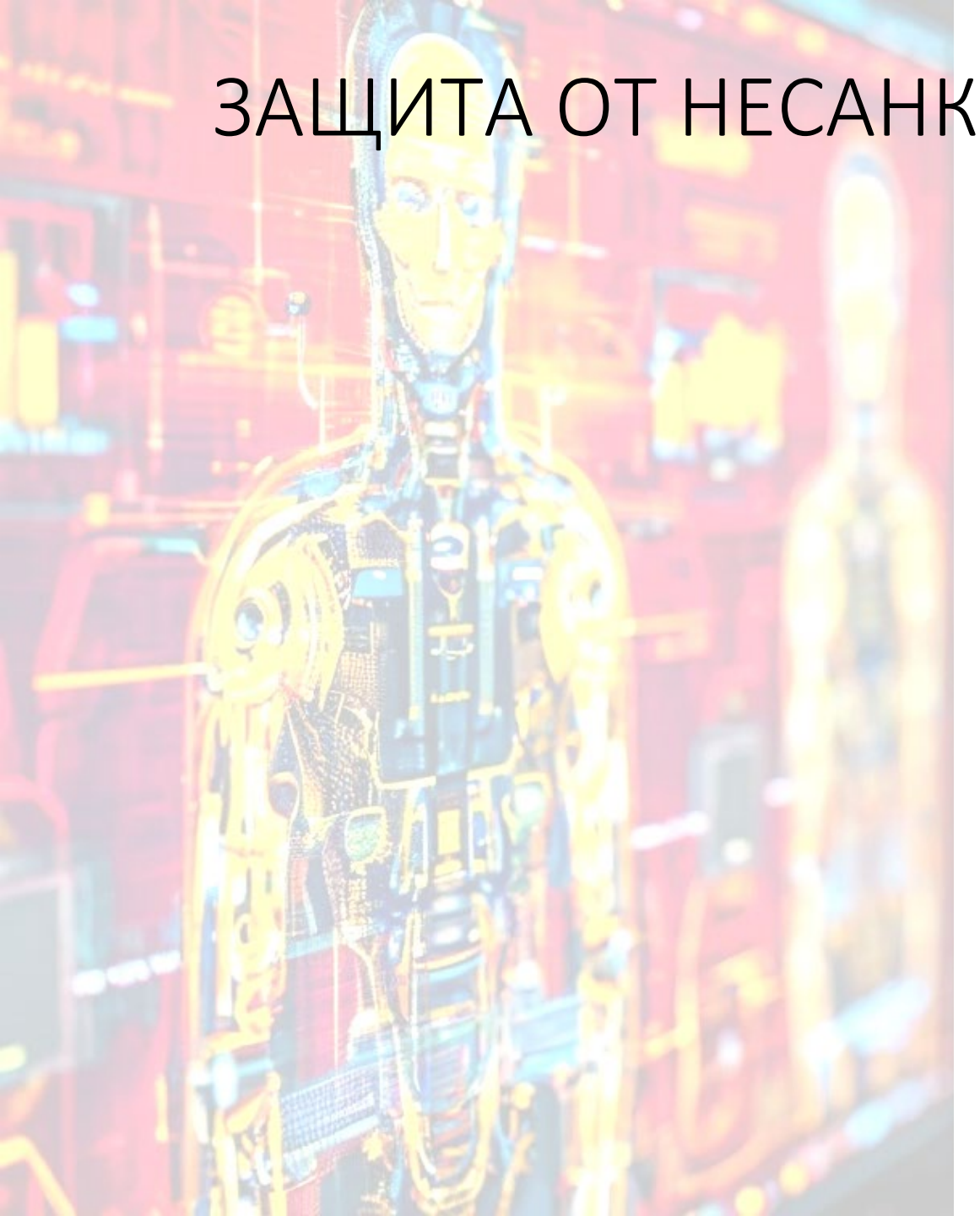
1. Защита компьютеров от НСД
2. Защищённые архитектуры компьютеров и компьютеры с «вирусным иммунитетом»
3. Защищённые загрузчики ОС и другие специальные инструменты
4. Доверенный ИИ – это целое большое направление с двумя ветвями:

    1) как сделать системы ИИ доверенными

    2) как использовать системы ИИ для обеспечения защиты информации

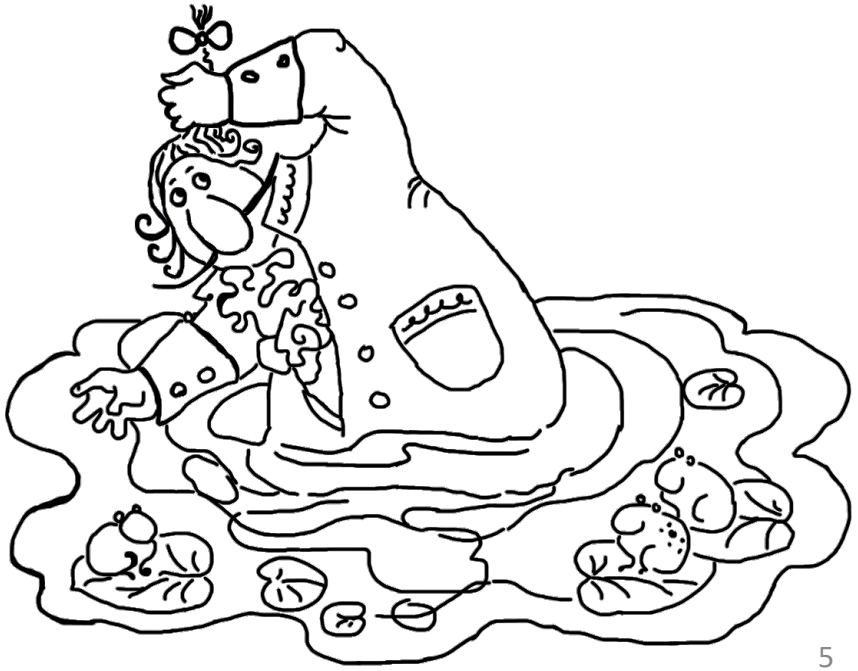
Это только примеры, а все направления собраны в большую таблицу, которую можно получить и прочитать.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

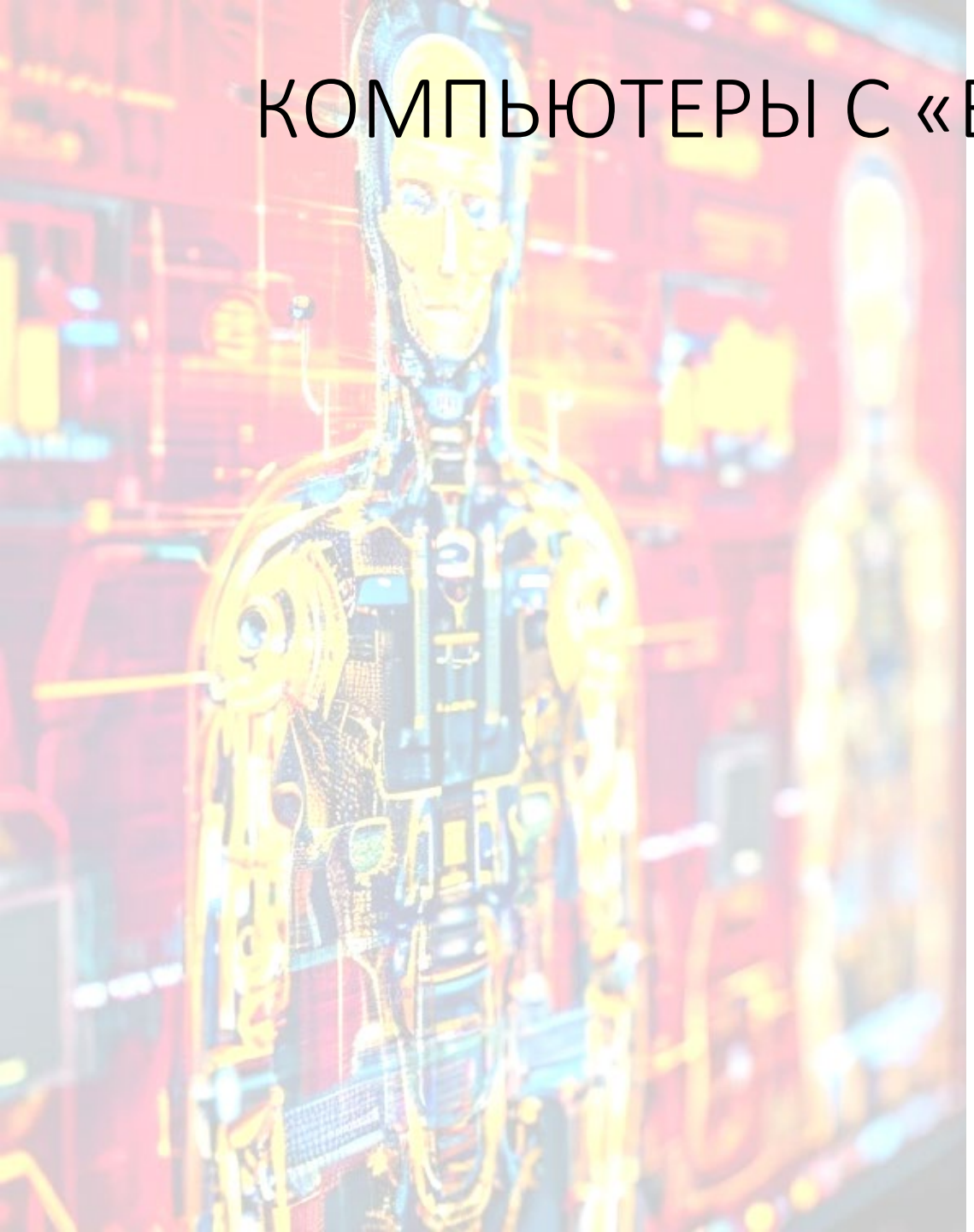


Уязвимость компьютеров – архитектурная, поэтому бесполезны программные средства, чтобы её исправить, нужен аппаратный резидентный компонент безопасности.

Это большое направление, так как их нужно множество разных – для разных задач.



КОМПЬЮТЕРЫ С «ВИРУСНЫМ ИММУНИТЕТОМ»



Компьютер может не иметь архитектурной уязвимости только в одном случае – если он имеет другую, защищённую архитектуру.

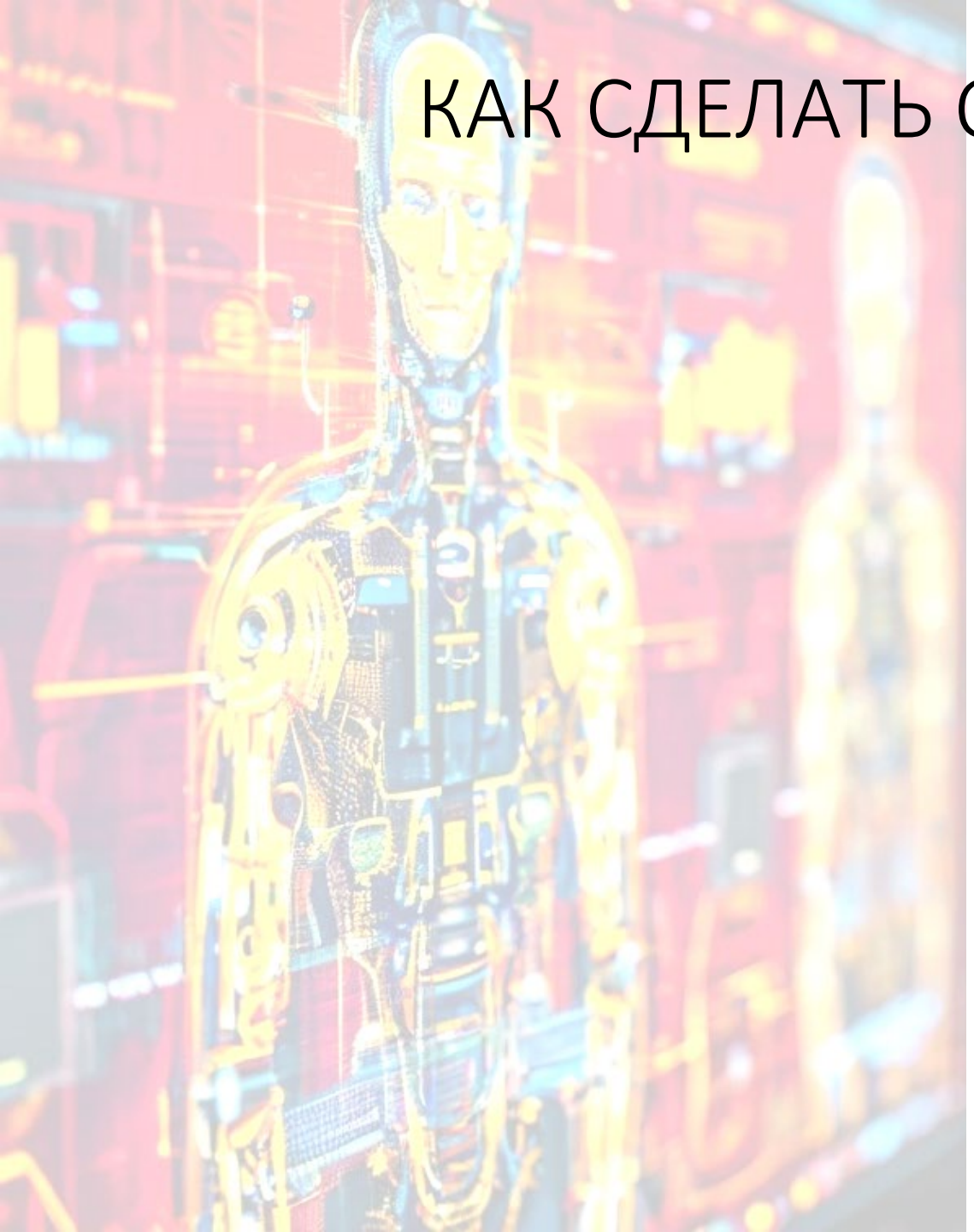
Такая архитектура называет Новая гарвардская, это наша разработка.

С развитием этой архитектуры и компьютеров с этой архитектурой связано множество инновационных задач.

СПЕЦИАЛЬНЫЕ ИНСТРУМЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ

- Защищённые загрузчики ОС
- Защищённые флешки
- Защищённые инструменты управления
- Защищённые загрузочные устройства
- Средства контроля UEFI
- Решения для защищённого дистанционного банковского обслуживания
- Рефлекторная биометрическая идентификация
- Инструменты защиты от дипфейков при идентификации по лицу

Задачи возникают каждый день. Нужно их решать.



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.

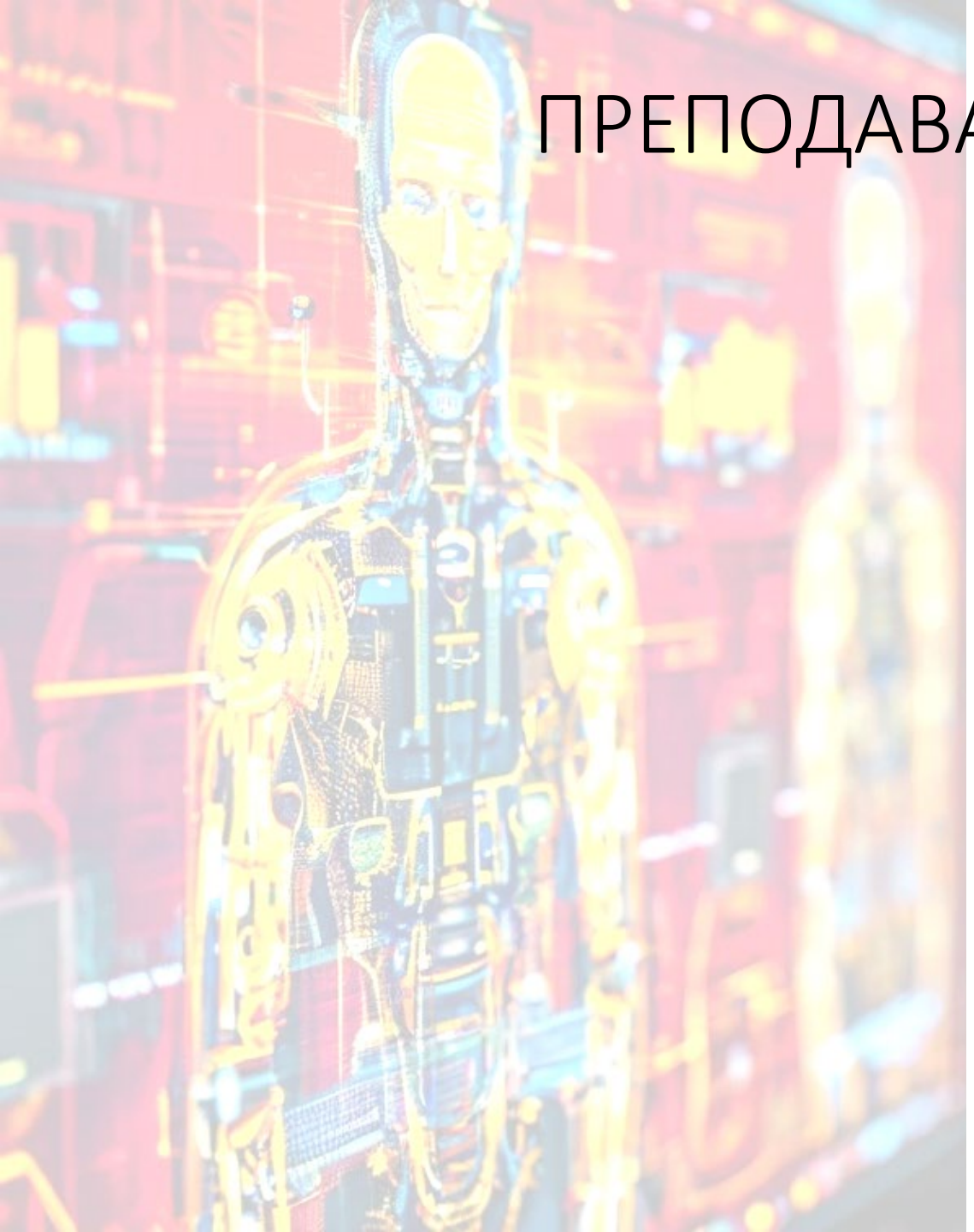
На текущем уровне развития науки и техники – это комплекс научных задач с перспективами инженерных решений.

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.

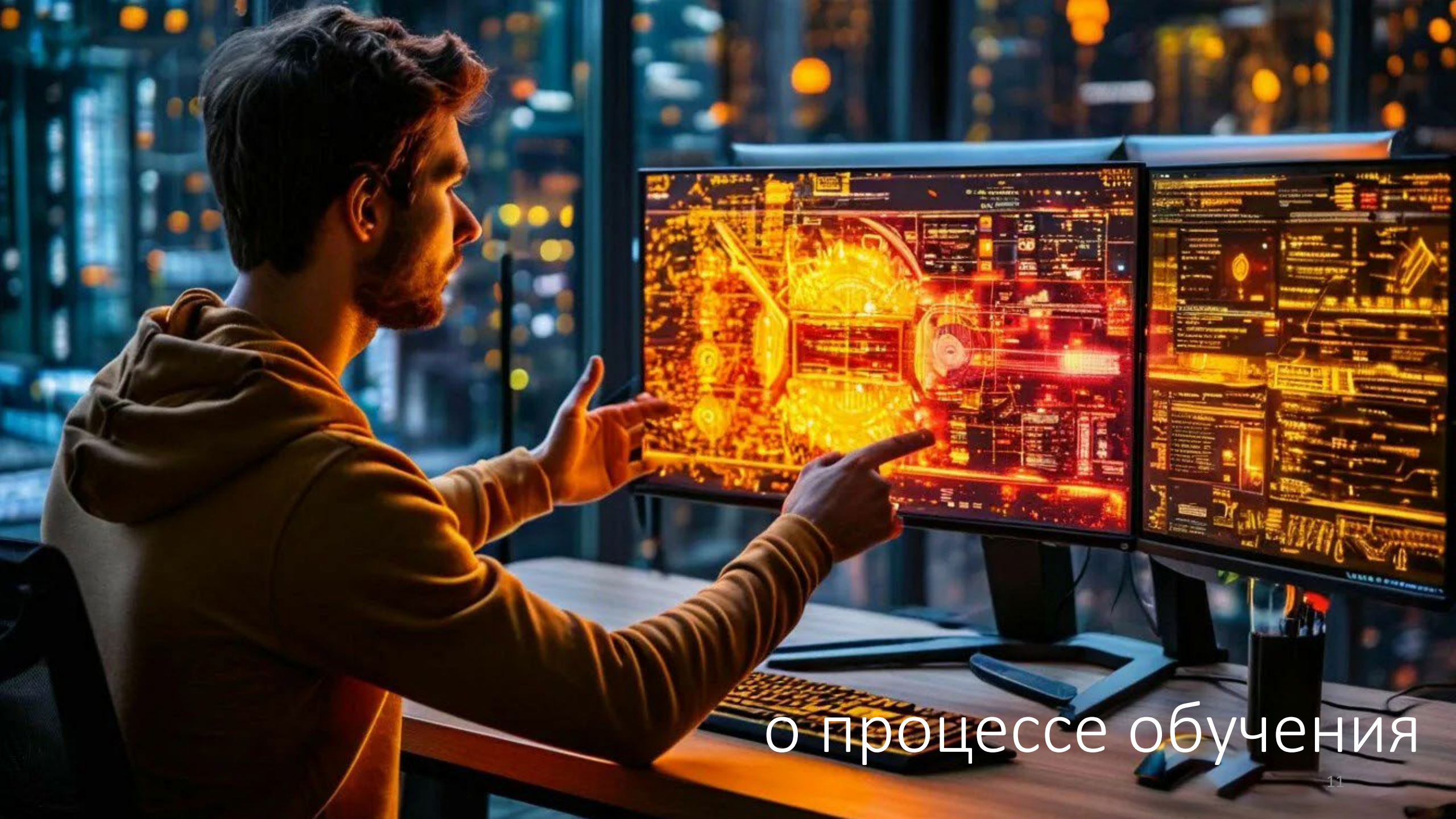


ПРЕПОДАВАТЕЛИ БАЗОВЫХ ДИСЦИПЛИН

Все базовые дисциплины кафедры 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.

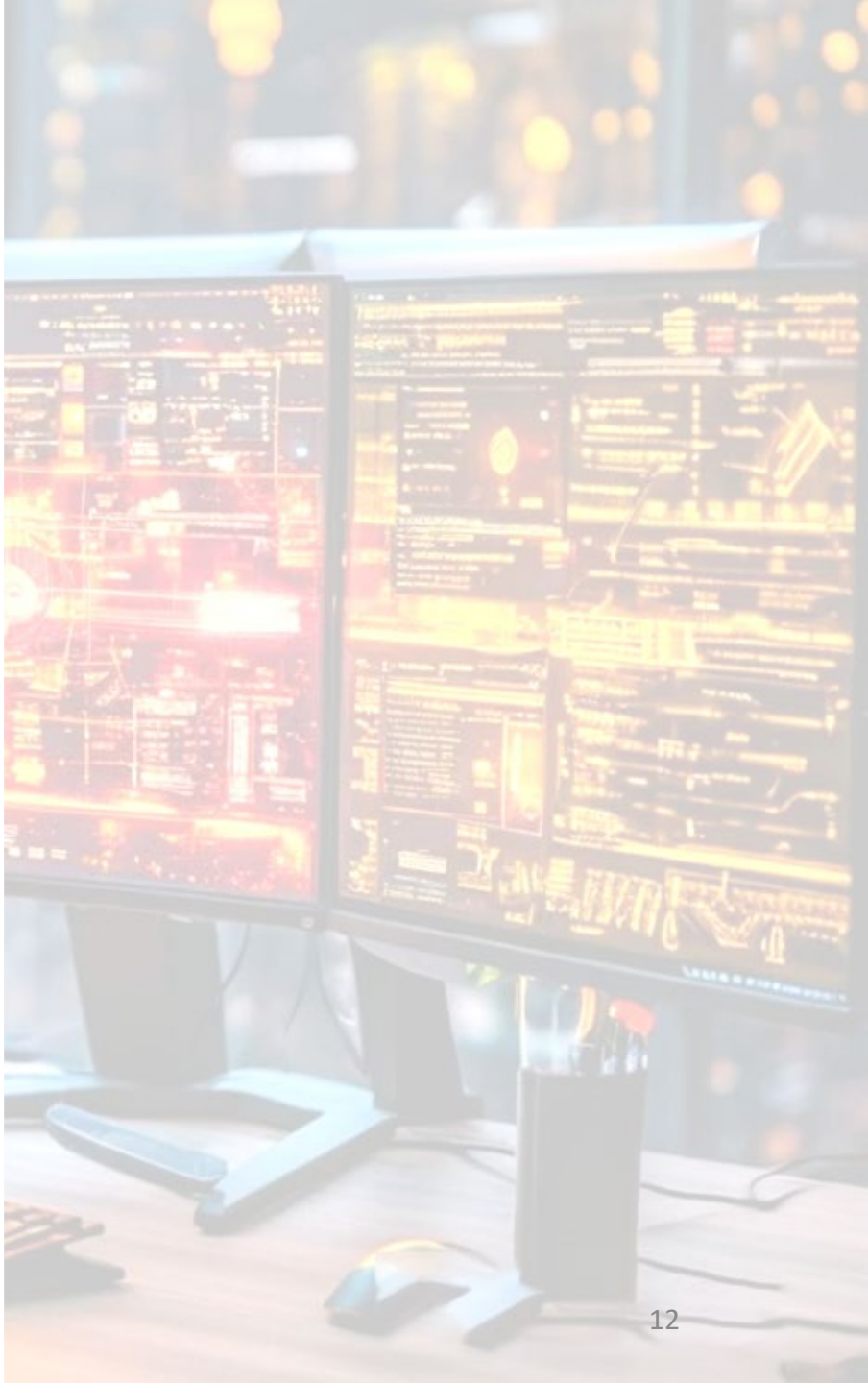
Именно они также руководят научно-исследовательскими работами.



о процессе обучения

СПИСОК БАЗОВЫХ ДИСЦИПЛИН

Курс	Семестр	Предмет	Преподаватель
3	Весенний	Введение в специальность	Конявский В.А.
4	Осенний, весенний	Программные средства доверенной загрузки	Алтухов А.А.
4	Осенний	Математические задачи в защите информации	Конявский В.А.
4	Осенний	Основы ОС Linux	Денисов Д.П.
4	Весенний	Средства защиты информации	Каннер Т.М.
4	Весенний	Программные средства разграничения доступа	Каннер А.М.
4	Весенний	Разработка документации при проектировании СЗИ	Сягаев Б.В.

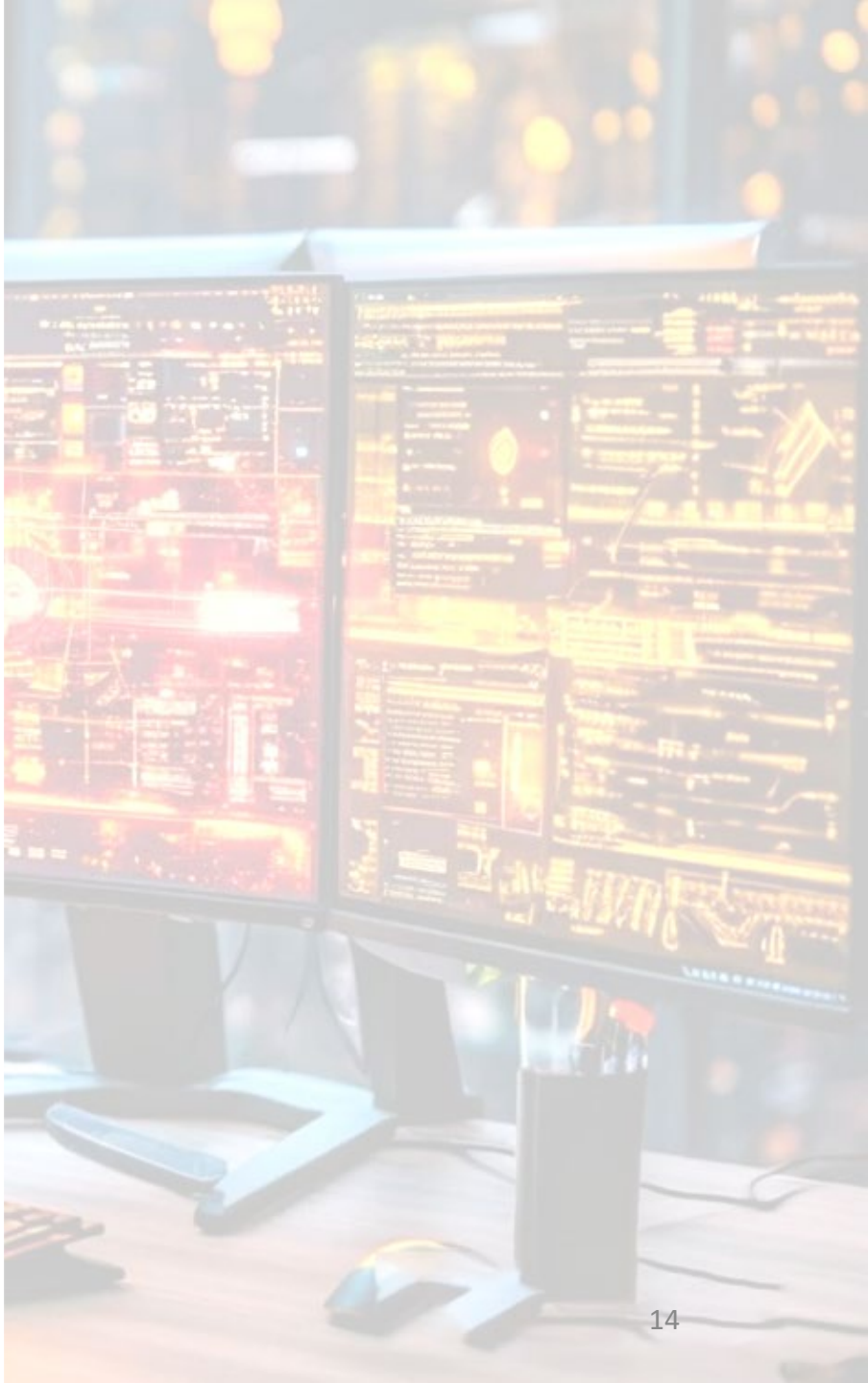


МЕСТО И ВРЕМЯ ЗАНЯТИЙ

Базовые дисциплины проходят в четверг (у 3 курса) и с понедельника по среду (у 4) в ОКБ САПР, в Москве, на Павелецкой.

МОЖНО РАБОТАТЬ

- Работа в базовой организации в период обучения – дополнительно оплачивается и обязательно связана с учебными дисциплинами.
- Рабочий график можно строить и менять с учетом потребностей обучения.
- Можно работать и в других организациях, работа именно в ОКБ САПР приветствуется, но не является обязательной.
- Возможно увольнение, если мы не сработались, без отчисления с кафедры.
- Возможно отчисление за низкие учебные результаты, в том числе – за неудовлетворительные результаты НИР, даже если студент работает в базовой организации.



о поступлении

ЖЕЛАТЕЛЬНЫЕ СКЛОННОСТИ

Обучение на кафедре будет приятнее тем,

- кто обладает конкретным мышлением
- кому нравится работать с материальными объектами – оборудованием, приборами, элементной базой и экспериментальными установками
- у кого есть способности и интерес к радиоэлектронике, программированию, конструированию

ДЛЯ ПОСТУПЛЕНИЯ ДОСТАТОЧНО

- числиться студентом Физтех-школы Радиотехники и Компьютерных технологий (ФРКТ)

- заполнить анкету по ссылке и получить доступ к таблице с темами и направлениями исследований на кафедре

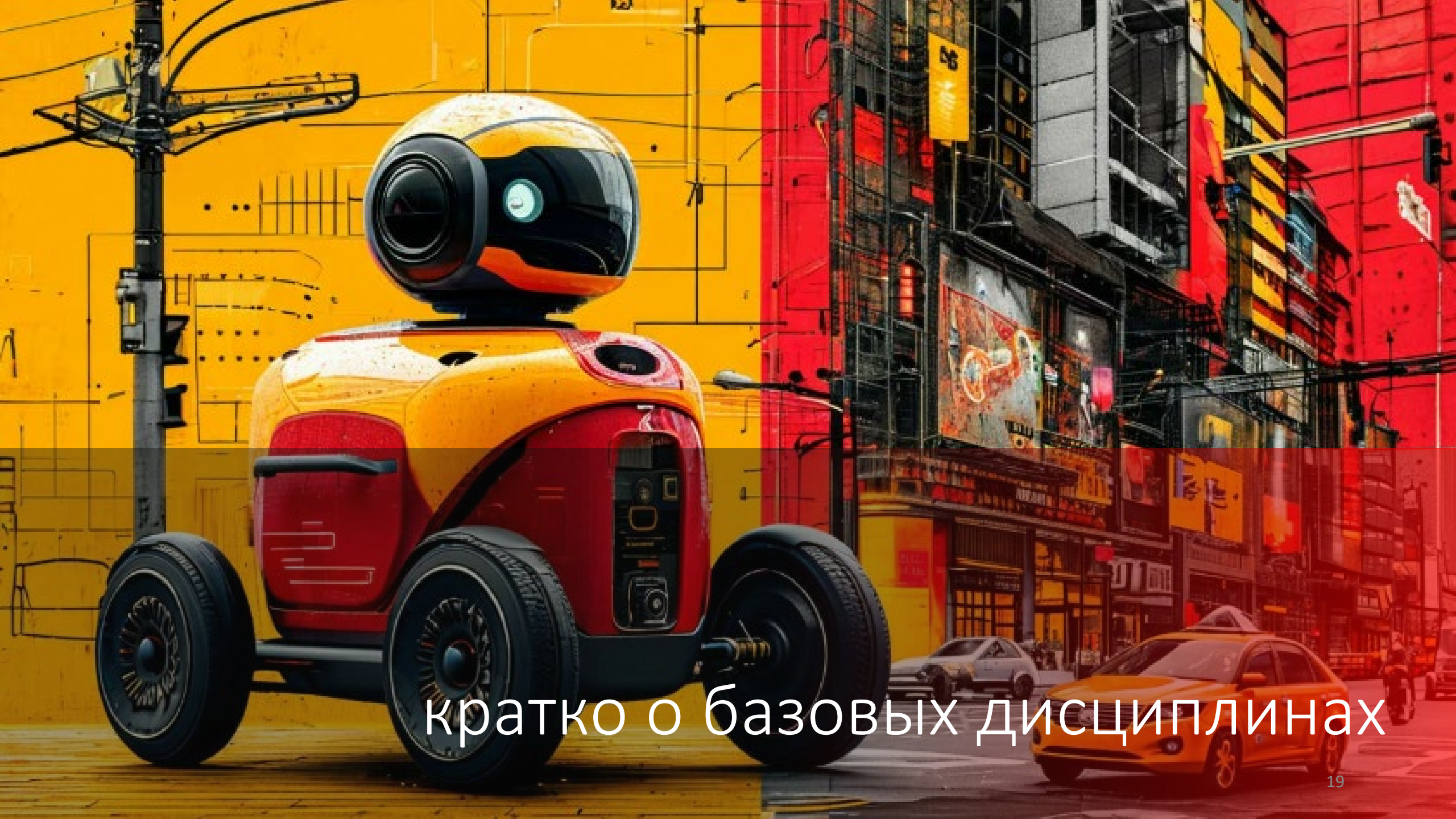
- если увидели, что это ваше, подать заявку в обыкновенном порядке с указанием кафедры защиты информации (конечно же, первым приоритетом ;))

- пройти собеседование на кафедре

ИИ ВАС ТОЧНО НЕ ЗАМЕНИТ

Главное, зачем вы идёте на эту специализацию?

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



кратко о базовых дисциплинах

Введение в специальность

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.

Программные средства доверенной загрузки

Узнаем

- методологические подходы к организации доверенных вычислений
- роль доверенной загрузки операционных систем в обеспечении их целостности и контролируемости
- концепции доверенной вычислительной среды, доверенной интеграционной платформы и резидентных компонентов безопасности
- методы разработки, анализа и исследования безопасности программных решений доверенной загрузки, включая методы анализа уязвимостей и реверс-инжиниринга прошивок

Научимся

разрабатывать, анализировать и оценивать программные компоненты систем доверенной загрузки, в том числе с учетом актуальных требований отечественных регуляторов в сфере информационной безопасности

Математические задачи в защите информации

Узнаем

- о современных методах и средствах защиты информации, основанных на применении классических математических задач
- о применении криптографии в реальных технических системах
- об использовании прикладной математики для выполнения требований регуляторов в части разработки и применения средств криптографической защиты информации,
- о видах криптографических преобразований и способах их применения

Научимся

применять математические методы и криптографические алгоритмы в задачах защиты информации и защищенных технических системах

Основы ОС Linux

Узнаем

- архитектуру Linux систем
- механизмы взаимодействия приложений с ядром операционной системы

Научимся

ключевым приёмам программирования на Си для Linux-систем

Практические занятия состоят из лабораторных работ

Средства защиты информации

Знакомство с современными средствами защиты информации.

Узнаем о существующих средствах защиты информации:

- универсальных защищенных флешках,
- носителях ключевой и аутентификационной информации,
- защищенных носителях вычислительной среды,
- защищенных носителях служебных данных,
- средствах обеспечения доверенной загрузки,
- средствах разграничения доступа.

Научимся

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

Программные средства разграничения доступа

Узнаем

- теоретические модели управления доступом
- практические механизмы управления доступом, являющихся фундаментом безопасности любой информационной системы

Научимся

самостоятельно конфигурировать операционные системы

Разработка документации при проектировании СЗИ

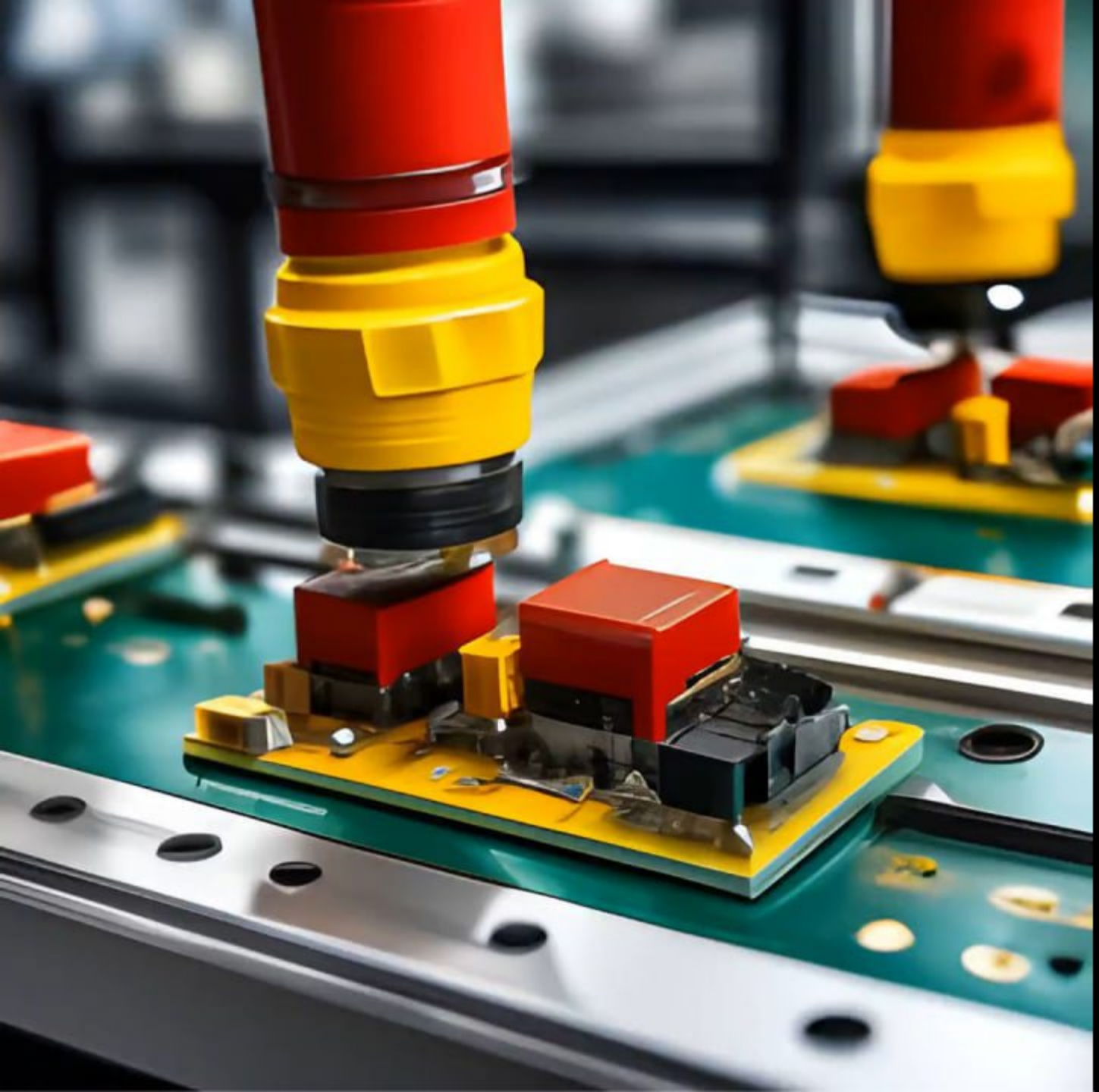
Узнаем

- положения национальных стандартов,
- положения нормативных документов ФСТЭК России, используемых при разработке средств защиты информации в программном и программно-техническом исполнении.

Основное внимание уделяется комплексу стандартов Единой системы программной документации (ЕСПД) и комплексу стандартов на разработку автоматизированных систем, содержащих, в том числе рекомендации по документальному оформлению результатов проектирования на каждой стадии разработки.

Научимся

Составлять и оформлять документы техно-рабочих проектов.



КОНТАКТЫ

Зам. зав. кафедрой (бакалавриат):

Хмельков Алексей Дмитриевич

khmelkov@phystech.edu

+7 (495) 994-72-62

анкета тут: