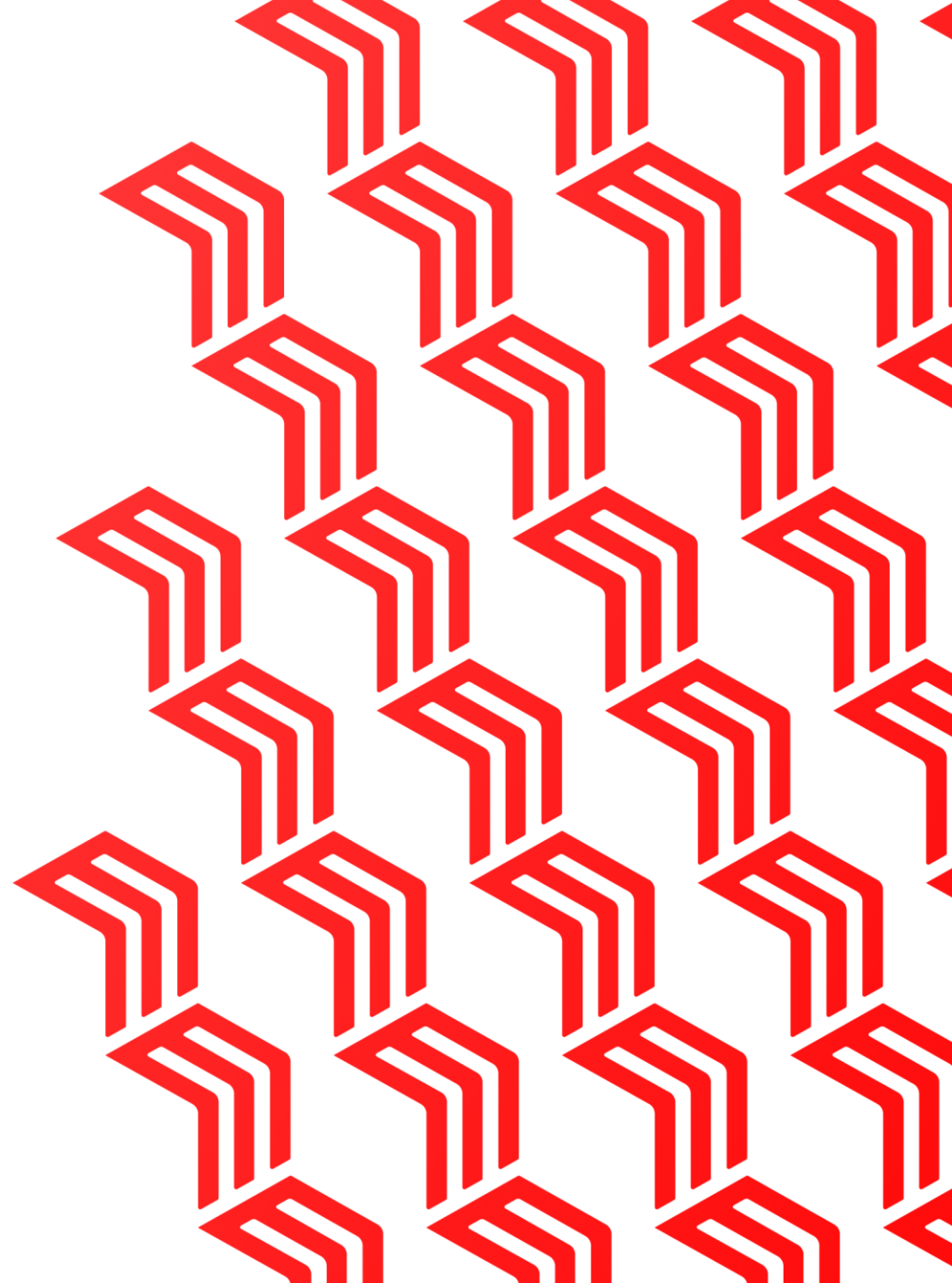


Проблемы и пути их решения в процессе подготовки кадров в области кибербезопасности с учетом влияния ИИ


Дмитрий Федоров,


руководитель направления по взаимодействию
с вузами, Positive Technologies

academic@ptsecurity.com





Дмитрий Федоров

 Руководитель направления по взаимодействию с вузами, Positive Technologies

 Старший преподаватель Высшей школы кибербезопасности СПбПУ

 Участник РГ по разработке первых профессиональных ИБ стандартов в 2016 году

 Автор учебника «Программирование на Python» (Юрайт, 6 издание),
онлайн курса «Язык программирования Python» (lektorium.tv/python)

 Автор канала «Кибербез образование» (t.me/cyber_edu) и подкаста



Обеспечиваем кибербезопасность

20⁺
лет

опыта исследований
и разработок

2,5⁺
тыс

сотрудников: инженеров
по ИБ, разработчиков,
аналитиков и других
специалистов

250⁺

экспертов в нашем
исследовательском
центре безопасности

200⁺

обнаруженных
уязвимостей
нулевого дня в год

250⁺

аудитов безопасности
корпоративных систем
делаем ежегодно

3⁺
тыс

клиентов из 10+ отраслей

- Создаем продукты и решения
- Проводим аудиты безопасности
- Расследуем инциденты
- Исследуем угрозы

■ **positive technologies**

 [О компании](#)

 [О продуктах компании](#)

Positive Education

Мы готовим лидеров, которые будут **защищать будущее**.

Профессионалам ИБ и ИТ показываем, как сделать кибербезопасность результативной, а топ-командам – как **определить ожидания** от ИБ и **измерить результат**.

Направления Positive Education

- Образовательные программы для профессионалов
- Обучение и сертификация по продуктам Positive Technologies
- Образовательно-стратегические сессии по погружению в кибербез для топ-команд
- Комплексные корпоративные программы
- Партнерство с вузами по подготовке кадров в сфере результативной кибербезопасности
- Онлайн-курсы для всех
- Развитие преподавателей по кибербезопасности

Глоссарий

Объекты информационной безопасности – антропоные системы:

- человек (тело, психика, сознание)
- корпорация (активы, персонал, руководство)
- государство (инфраструктура, население, власть)

Цель обеспечения информационной безопасности субъекта – предотвратить (минимизировать) причинение вреда субъекту путём информационного воздействия на него и/или деструктивного воздействия на информационные ресурсы, необходимые для формирования у него корректного мировоззрения и корректной методологии.

Объекты кибербезопасности – информационно-кибернетические системы

Цель защиты информационных ресурсов (кибербезопасности) субъекта – предотвратить (минимизировать) причинение вреда субъекту и/или третьим лицам в результате некорректного использования или деструктивного воздействия на информационную инфраструктуру и информационные ресурсы субъекта.

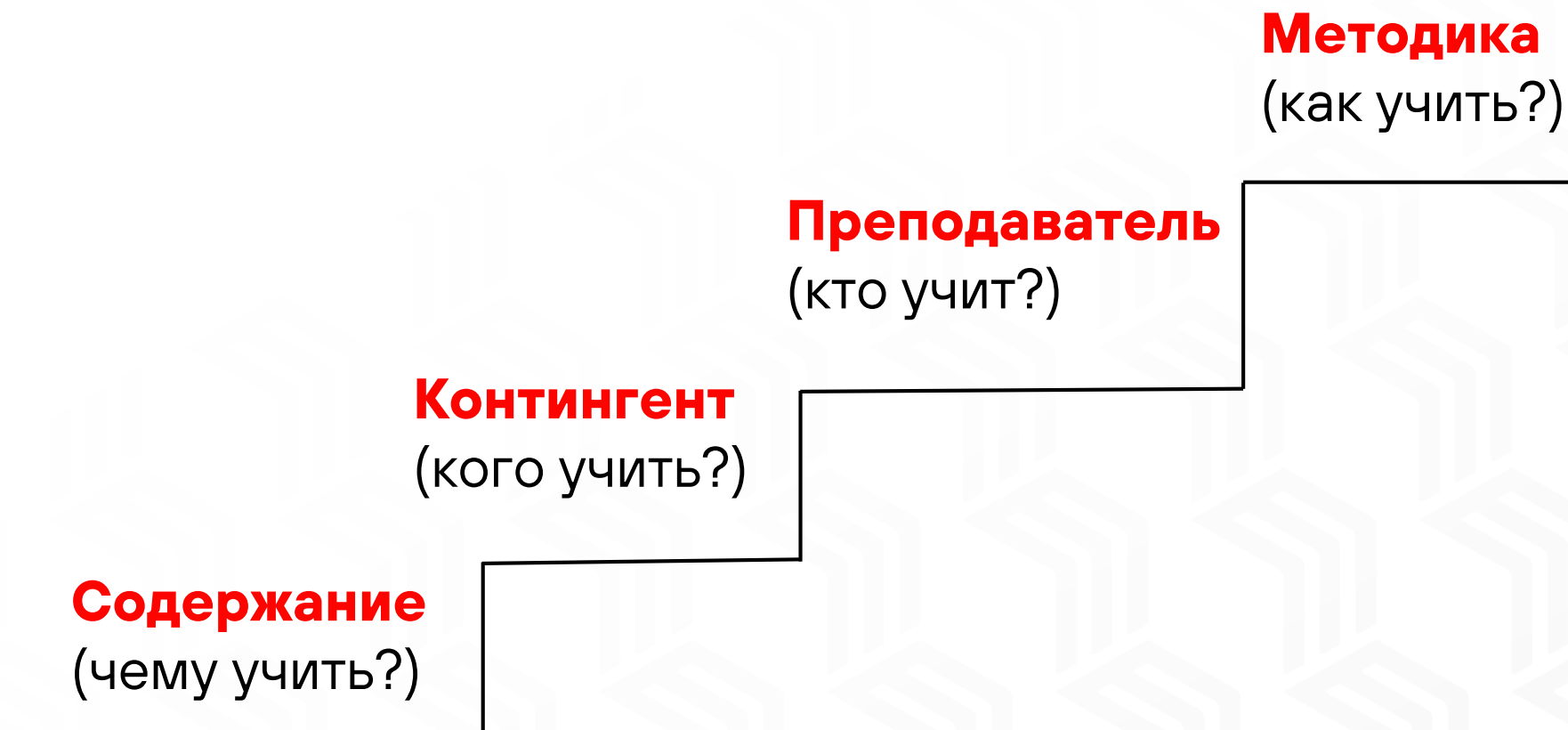


Термины и определения в
области кибербезопасности
(cybersecurity-glossary.ru)

Что происходит с выпускниками по ИБ/КБ?

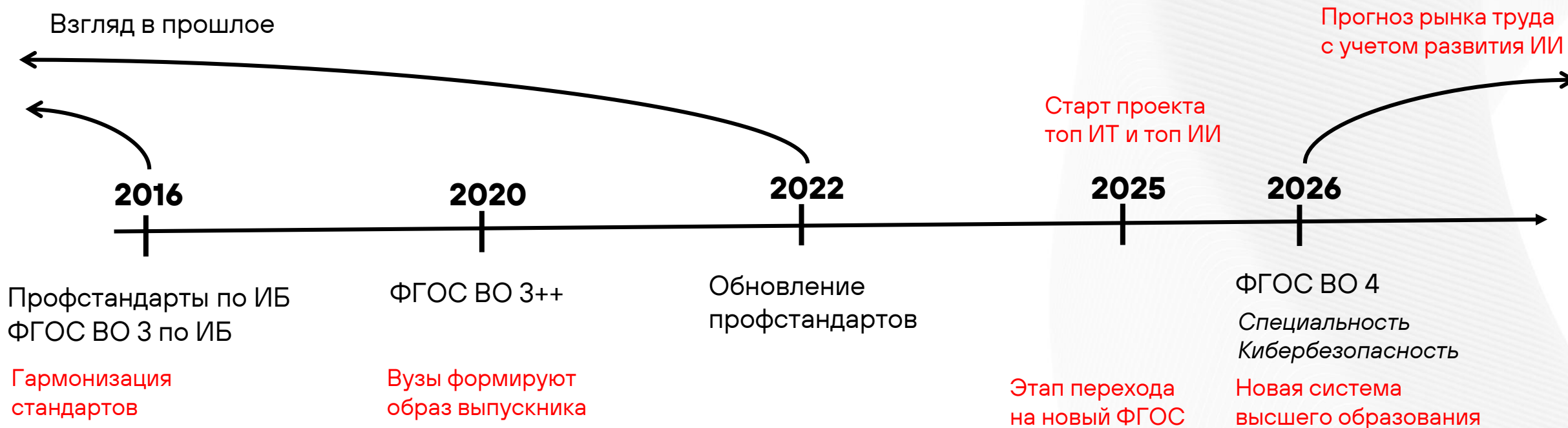


Схема выступления



Содержание (чему учить?)

Профстандарты не отражают в полной мере кадровой потребности отрасли



ПЕРЕХОД ОТ КОМПЕТЕНТНОСТНОЙ МОДЕЛИ ПО НАПРАВЛЕНИЯМ ПОДГОТОВКИ К КАТЕГОРИЙНО-РОЛЕВОЙ КОМПЕТЕНТНОСТНОЙ МОДЕЛИ

КАТЕГОРИИ ИИ-СПЕЦИАЛИСТОВ:

Специалист экстра-класса

(исследователь/креативный разработчик ИИ)

Массовый разработчик ИИ-решений

Отраслевой ИИ-специалист

Отраслевой специалист –

квалифицированный заказчик и потребитель ИИ

Специалист по развитию экосистемы ИИ

(этика, конфликтология и пр.) будут в 2028-2030

ПРОФЕССИОНАЛЬНЫЕ РОЛИ:

- AI CDO
- AI Architect
- AI PM
- ML Researcher
- ML Engineer
- AI Security Engineer
- Data Architect
- Data Analyst
- Data Engineer
- Tech analyst DS
- MLOps
- Domain ML Specialist
- AI Operator
- AI Qualified Customer

ПОКРЫТИЕ ПРОФЕССИОНАЛЬНЫХ РОЛЕЙ ПО КАТЕГОРИЯМ ИИ-СПЕЦИАЛИСТОВ

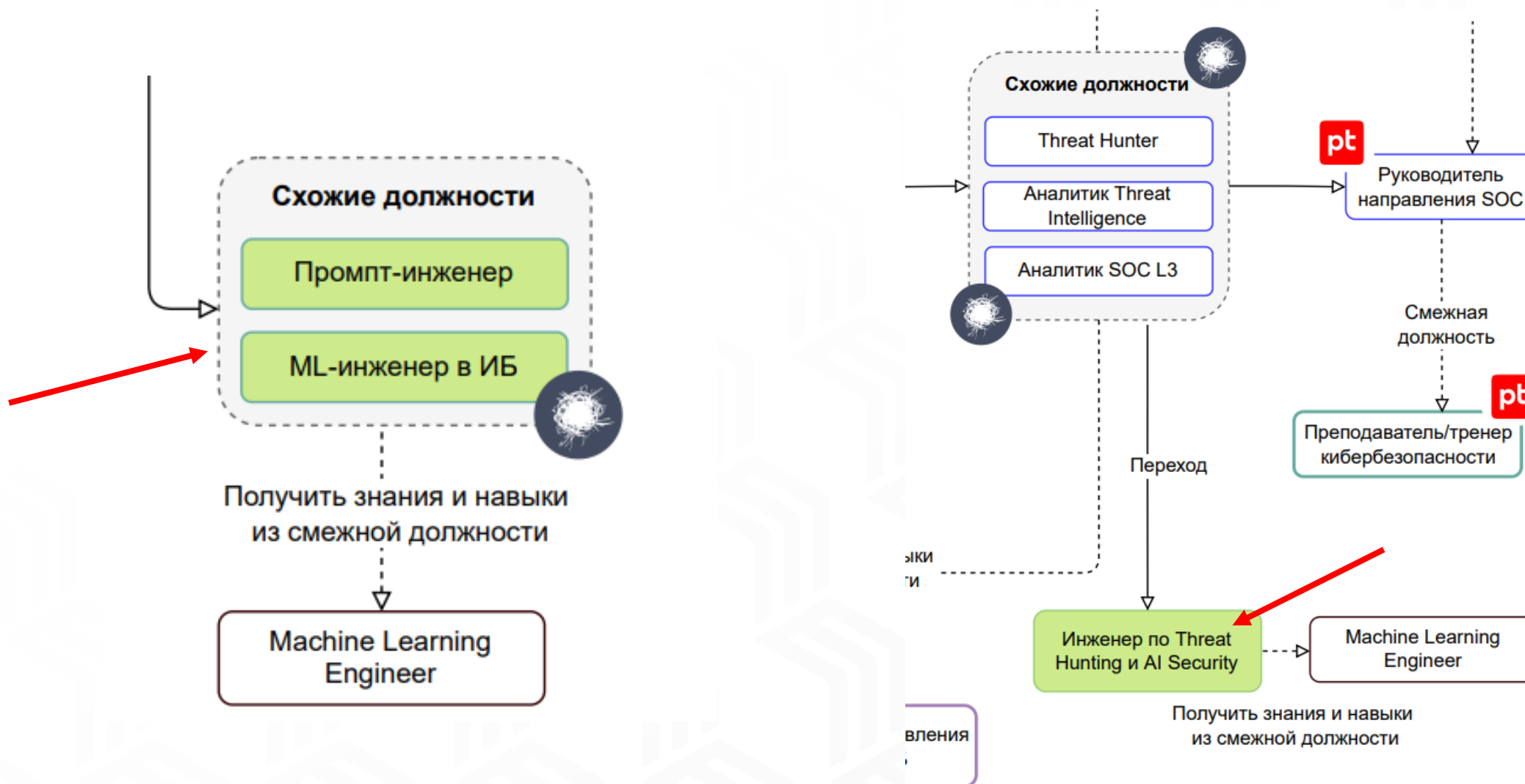
Категория	AI CDO	AI Architect	AI PM	ML Researcher	ML Engineer	AI Security Engineer	Data Architect	Data Analyst	Data Engineer	Tech analyst DS	MLOps	Domain ML Specialist	AI Qualified Customer	AI Operator
ИИ-специалист экстра-класса		✓		✓			✓	✓						
Массовый разработчик ИИ			✓	✓	✓	✓	✓	✓	✓	✓				
Отраслевой ИИ-специалист	✓		✓				✓	✓	✓	✓	✓	✓	✓	✓
Заказчик и потребитель ИИ	✓		✓										✓	✓

**Специалист по кибербезу
попадает в эту категорию**

Предлагаемая схема работы



Появление должностей, связанных с ИИ



О схеме карьерных треков

Терминология в
кибербезопасности

Обязательные знания и
навыки в кибербезе

Основные концепции
кибербезопасности

Подкаст “Беседы про
кибербез образование”

Примерные темы
студенческих работ по
кибербезу

Вузы по ИБ на карте

Должности и
специализации в
кибербезопасности

AppSec-инженер

Cloud Security инженер

Compliance аналитик

DevSecOps

MLSecOps-инженер

ML-инженер в ИБ

Security Champion

Аналитик SOC L1

Аналитик SOC L2

Аналитик SOC L3

Аналитик киберугроз

Аналитик-исследователь

Аналитик SOC L1

Обязанности

- Мониторинг событий безопасности, полученных с помощью оповещений SIEM или других инструментов безопасности;
- Обработка инцидентов, поступающих от пользователей через email и заявки;
- Назначение начальных приоритетов для входящих сообщений (начальная оценка приоритетов событий, определение инцидентов ИБ, определение потенциального риска и урона или эскалация запроса в соответствующие подразделения);
- Мониторинг состояния потенциальных инцидентов и соответствующих им зависимостей;
- Уведомление L2 об инцидентах с высоким приоритетом;
- Эскалация инцидентов на L2;
- Мониторинг очереди инцидентов;
- Мониторинг и эскалация ложноположительных срабатываний на технический отдел;
- Знание текущей политики реагирования на инциденты;
- Участие в программе Bug Bounty, разбор уязвимостей, реагирование на уязвимости, постановка задач на устранение
- Выявление и анализ инцидентов ИБ с использованием SIEM и других инструментов мониторинга инцидентов;
- Формирование предложений логики сценариев SIEM;
- Подготовка отчетных выгрузок о состоянии ИБ;
- Полный цикл ведения инцидентов в IRP – системе (регистрация, обработка, перевод, завершение инцидента, обработка false positive);
- Анализ дашбордов на выявление аномалий, мониторинг работоспособности SIEM;
- Прием обращений работников по подозрениям на инциденты ИБ;
- Проверка ПО в изолированных средах на наличие вредоносного содержимого с помощью автоматизированных СЗИ;
- Анализ и реагирование на инциденты информационной безопасности;
- Эксплуатация систем класса SIEM, NTA, WAF;

**Описание
должности**



Должности

Структура компетенции по кибербезопасности

Анализ вредоносных программ

Субъект

Младший или старший курсы программы бакалавриата по кибербезопасности.

Предварительные условия

Знание ассемблера x86, x64; знания в направлении реверс-анализа.

Поведение

Рабочая роль (должность): [вирусный аналитик](#)

Должность

Задача

Выполнение анализа вредоносного ПО.

Задача

Контекст

Сценарий: выступая в качестве аналитика вредоносных программ, при наличии нескольких файлов студент использует базовые методы анализа, включая сканирование на вирусы, статический и динамический анализ, для определения возможных вредоносных файлов.

Компетентность — это способность студента выполнять задачу в контексте должности (рабочей роли).

В отличие от абстрактных описаний знаний и навыков, компетентность относится к наблюдаемому выполнению действия, в конкретном (и часто смоделированном) контексте рабочего места.

КОНТИНГЕНТ (кого учить?)

МОДЕЛЬ ПОДГОТОВКИ ИИ СПЕЦИАЛИСТОВ ЭКСТРА КЛАССА И МАССОВЫХ РАЗРАБОТЧИКОВ ИИ

Классическая модель подготовки кадров в ИИ

КУРС 1-2

Общепрофессиональная фундаментальная подготовка (математика, основы ИТ)

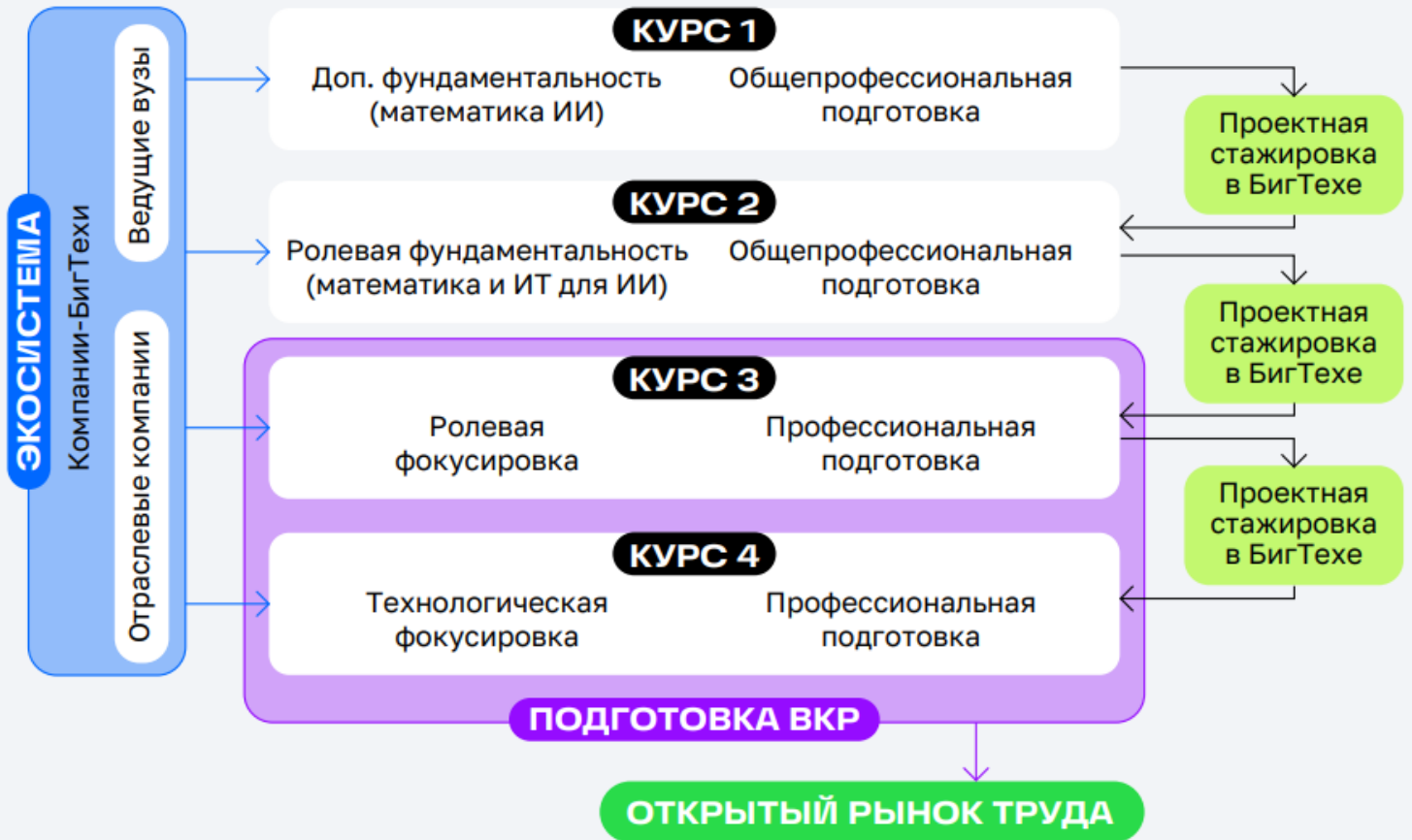
КУРС 3-4

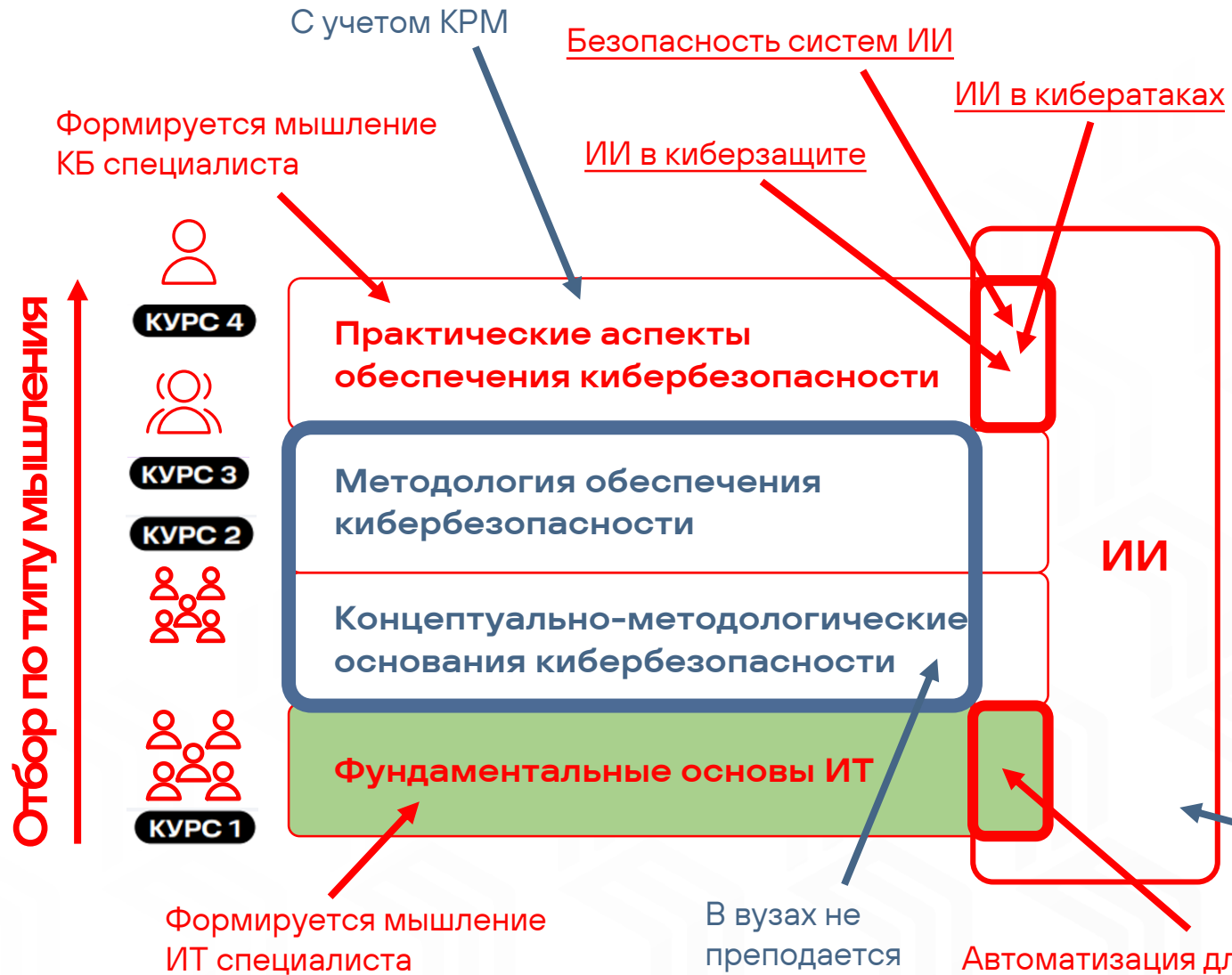
Профессиональная подготовка в рамках специализаций

Подготовка ВКР

ОТКРЫТЫЙ РЫНОК ТРУДА

Новая модель подготовки кадров в ИИ



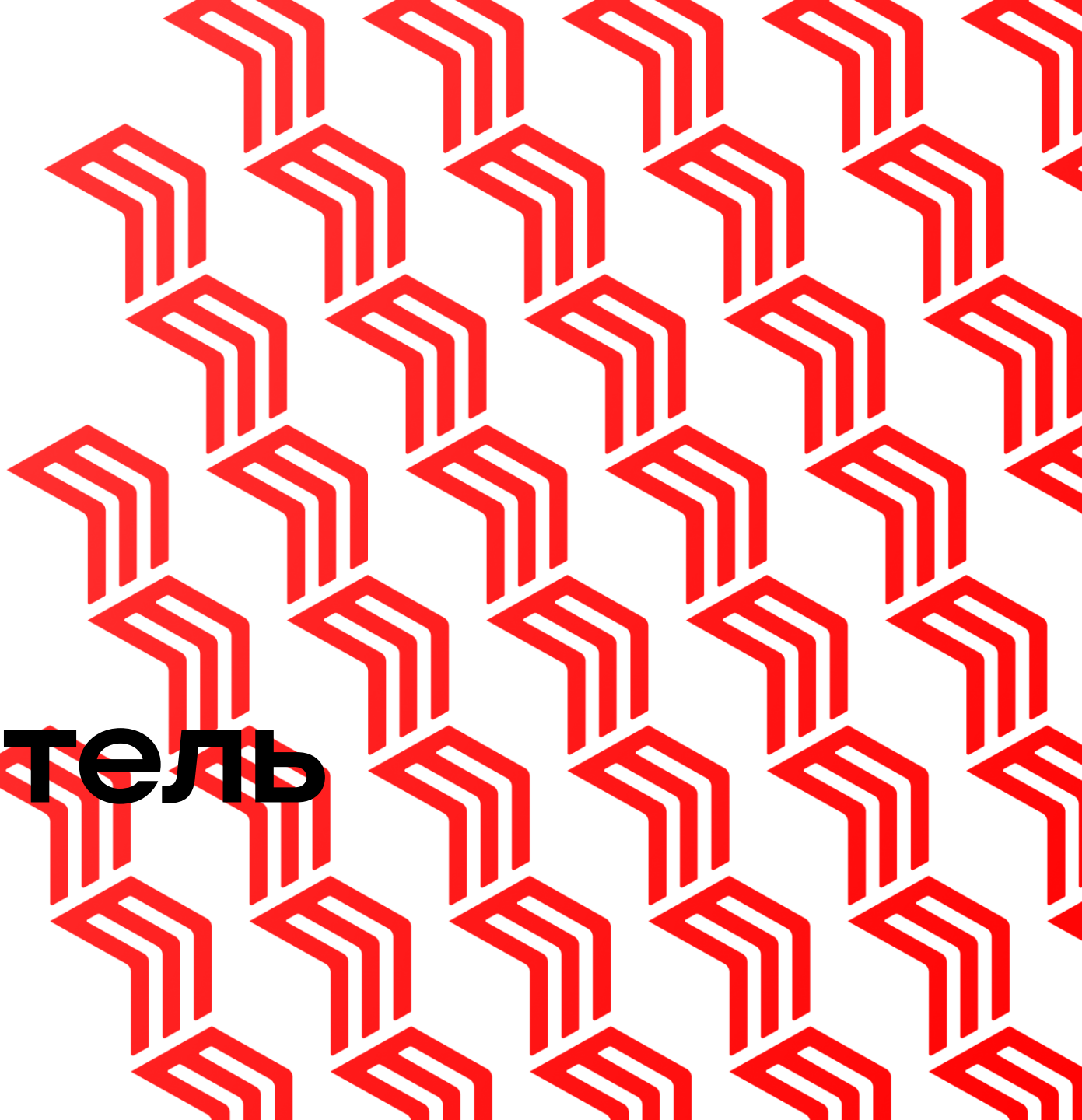


КБ требует особого типа мышления

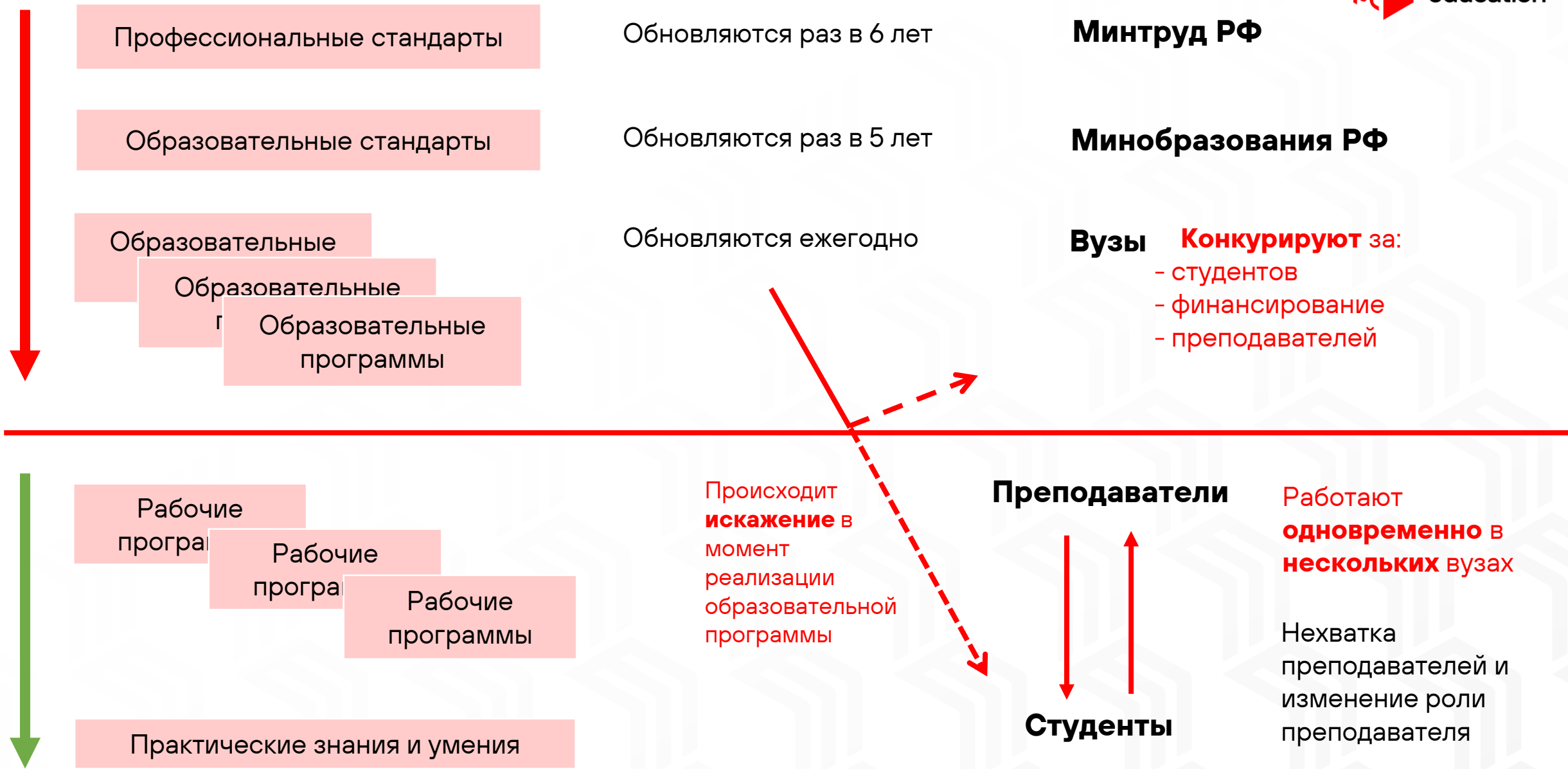
“Такое мышление неестественно для большинства людей. Оно неестественно для инженеров. Хорошая инженерия подразумевает размышления о том, как можно заставить систему работать; образ мышления в области безопасности подразумевает размышления о том, как можно заставить систему сломаться. Оно подразумевает мышление злоумышленника. Вам не нужно использовать уязвимости, которые вы находите, но если вы не смотрите на мир таким образом, вы никогда не заметите большинство проблем безопасности”.

(Брюс Шнайер)

Преподаватель (кто учит?)

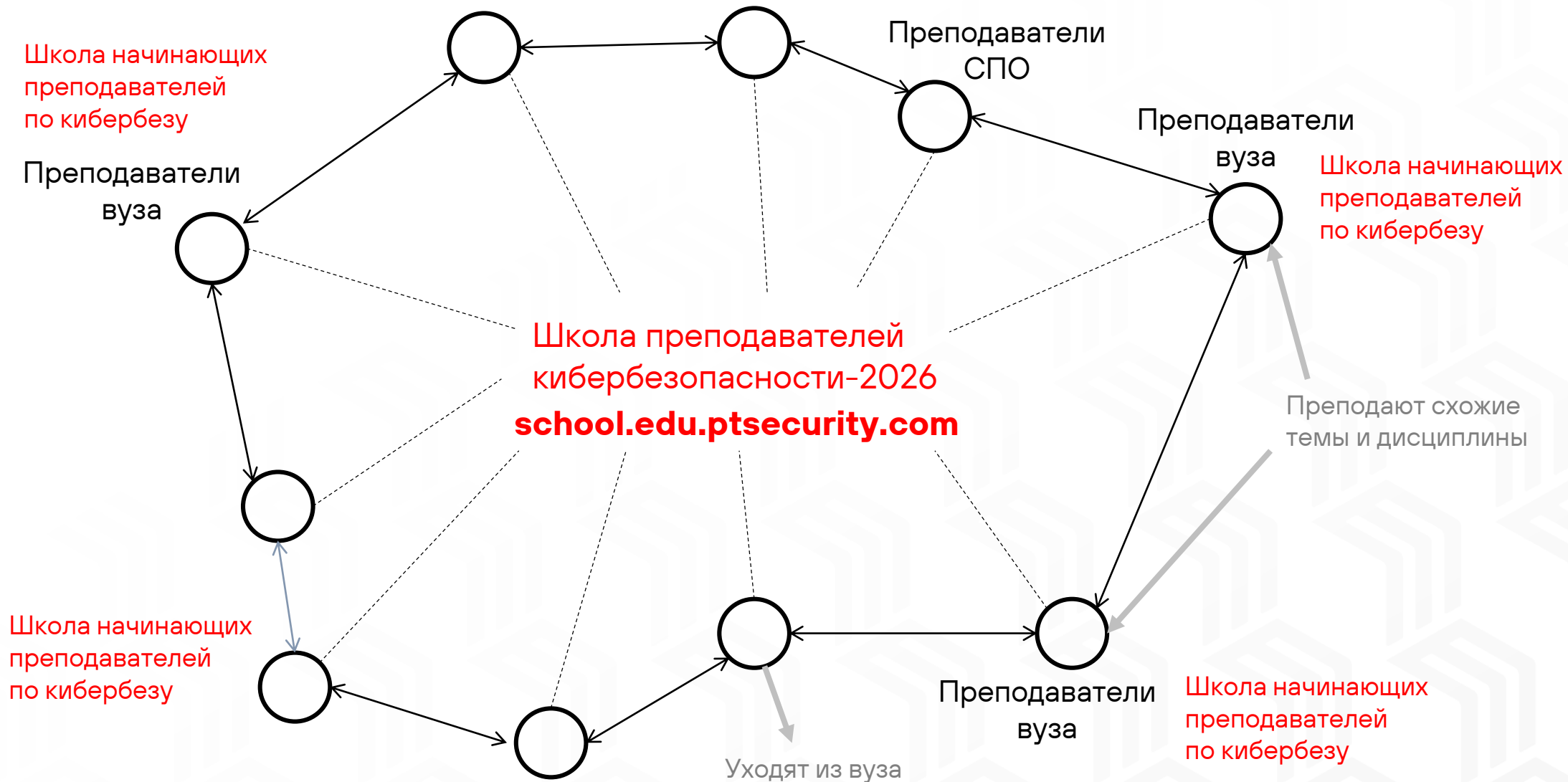


Управление системой образования на уровне страны



Реализация образовательной программы в вузе

410 образовательных организаций по ИБ/КБ в перспективе составляют сообщество преподавателей



Выпускной Школы преподавателей кибербезопасности 2025 на PHDays в Лужниках



Школа преподавателей кибербезопасности: ИТОГИ первого потока

Как ШПК и Бауманка учат преподавателей кибербезопасности

Удостоверение о повышении квалификации МГТУ им. Н.Э. Баумана получили более 300 преподавателей и учителей

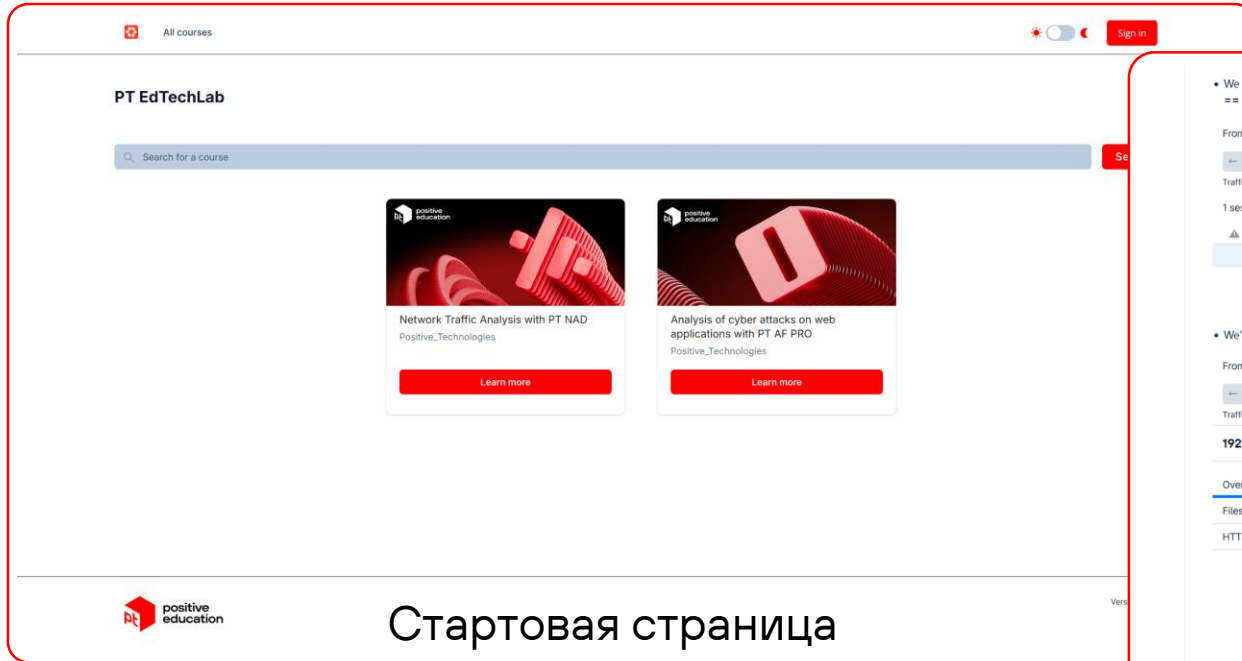
Методика (как учить?)



Кибертренажер PT EdTechLab



Автономное обучение снижает нагрузку на преподавателя и меняет его роль в учебном процессе



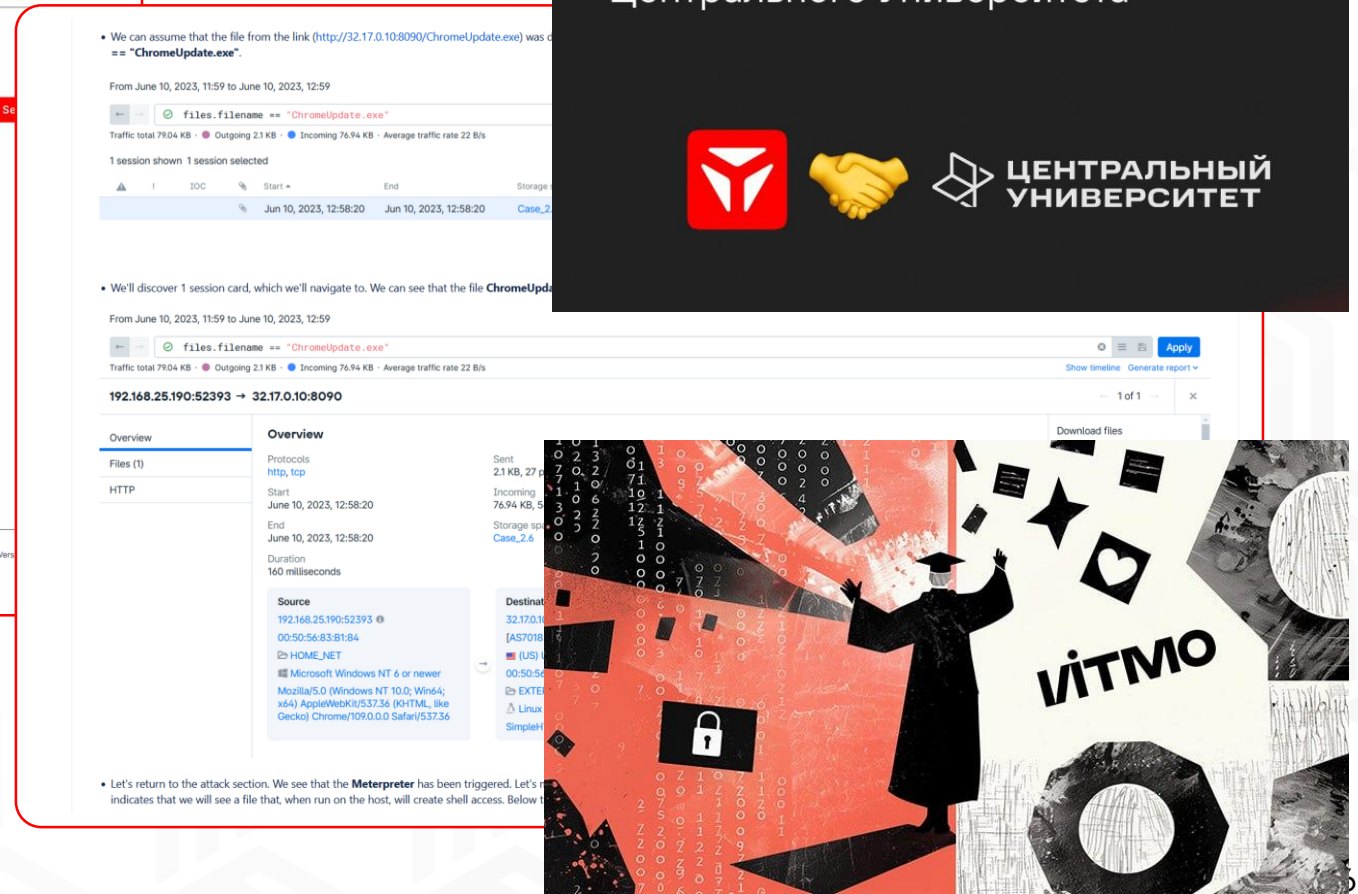
Стартовая страница

edu.ptsecurity.com/pt_edtechlab

Обучение специалистов через практику: как мы внедрили тренажёр PT EdTechLab в программу курса Центрального Университета



ЦЕНТРАЛЬНЫЙ
УНИВЕРСИТЕТ



Спасибо за внимание!

Дмитрий Федоров,

руководитель направления по взаимодействию
с вузами, Positive Technologies

academic@ptsecurity.com

