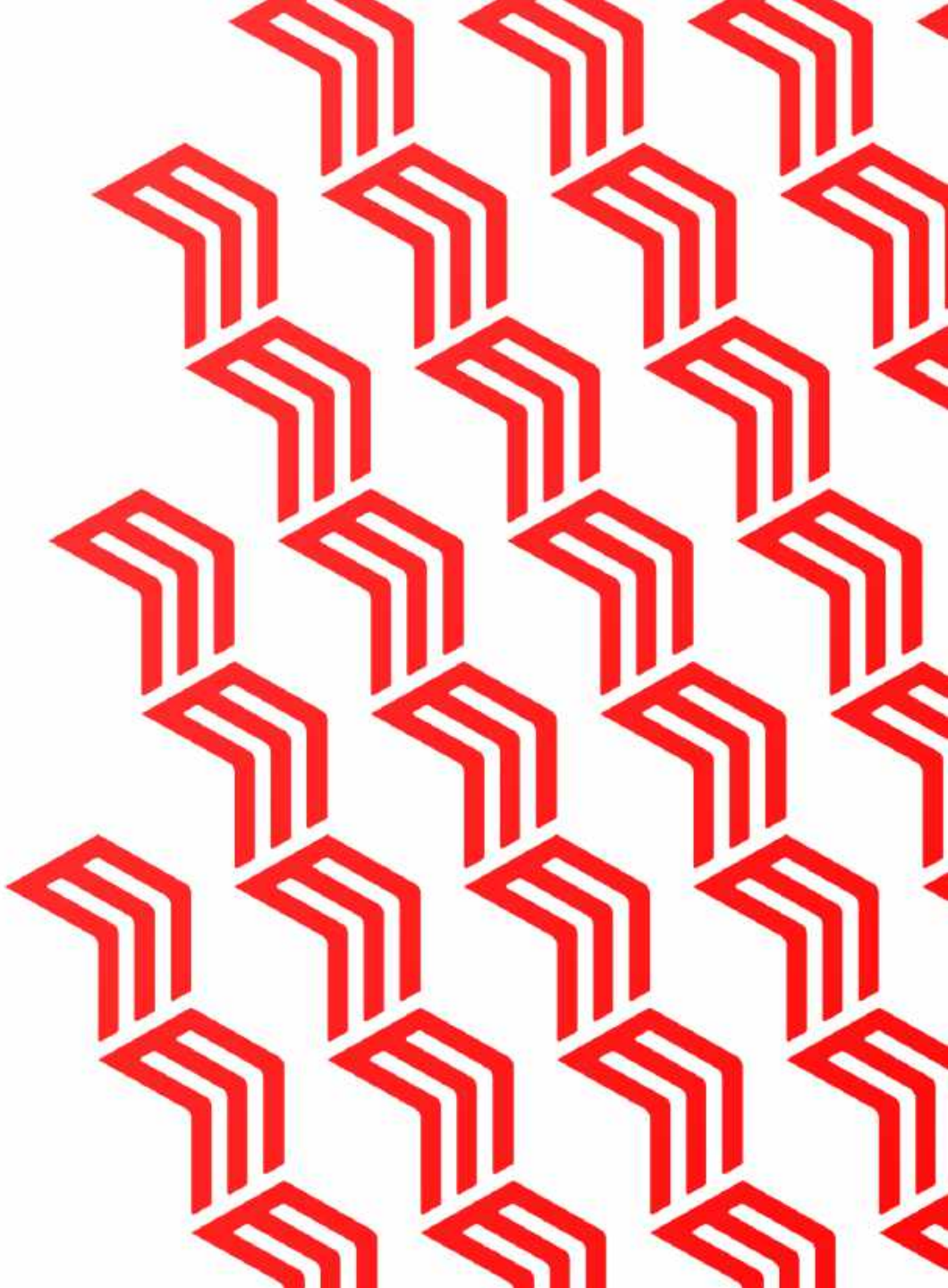
positive education

Подготовка специалистов по кибербезопасности в современных условиях

Дмитрий Федоров

Руководитель образовательных проектов,
Positive Technologies

edu.ptsecurity.com



Дмитрий Федоров

- Руководитель проектов по взаимодействию с вузами, Positive Technologies
- С 2010 года преподаю в вузах, руководил отделом по анализу данных, в настоящее время преподаватель СПбПУ (Институт кибербезопасности)
- Автор учебника «Программирование на Python» (Юрайт, 6 издание),

  онлайн курса «Язык программирования Python» (lektorium.tv/python)
- Автор канала «Кибербез образование» (t.me/cyber_edu)

Обеспечиваем кибербезопасность

20+ лет
опыта исследований и разработок

1,5+ 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

50%
всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

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

positive technologies

О компании

О продуктах компании

Positive Education

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

Мы хотим развивать рынок образования в кибербезе (Positive Research)

edu.ptsecurity.com

Комплексные практикумы

positive education

Генеральный директор

- Соблюдает принципы личной кибербезопасности
- Знает ключевые принципы кибербезопасности и актуальные угрозы КБ для организации

Директор

Начальник отдела

- Соблюдает принципы личной кибербезопасности
- Умеет внедрять результативную кибербезопасность в процессы компании
- Знает сценарии реализации кибератак и способы их предотвращения

Инженер ИБ

- Соблюдает принципы личной кибербезопасности
- Умеет эксплуатировать продукты Positive Technologies в боевых условиях

План выступления

- Современные условия подготовки специалистов по кибербезу
- Схема карьерных треков в кибербезе
- Кибербезопасность – специализация в ИТ
- Кибертренажер PT Education Technology Laboratory

01

positive education

Современные условия подготовки специалистов по кибербезу

Что происходит?

Управление системой образования на уровне страны

positive education

Профессиональные стандарты — Обновляются раз в 6 лет — **Минтруд РФ**

Образовательные стандарты — Обновляются раз в 5 лет — **Минобразования РФ**

Образовательные программы — Обновляются ежегодно — **Вузы**

Конкурируют за:
- студентов
- финансирование
- преподавателей

Происходит **искажение** в момент реализации образовательной программы

Преподаватели

Работают **одновременно** в **нескольких** вузах

Нехватка преподавателей и изменение роли преподавателя

Студенты

Рабочие программы

Практические знания и умения

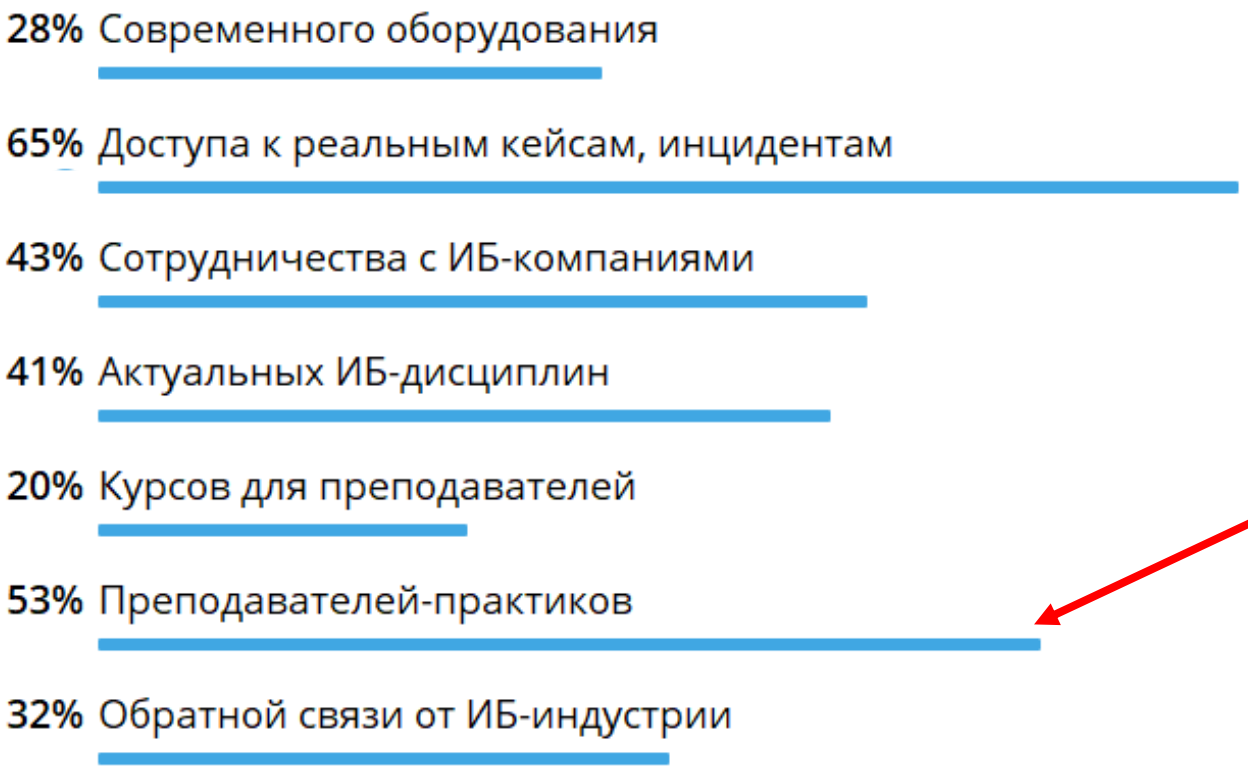
Реализация образовательной программы в вузе

positive education

Кибербез образование

Чего, на ваш взгляд, не хватает в образовательном процессе по кибербезу?

Результаты



377 голосов

Не хватает практики от практиков

Можно ли найти столько практиков в масштабах страны?

К решению этой задачи подключилось Минцифры:

- программы топ-уровня
- принуждение ИТ-компаний

Варианты сотрудничества компаний и вузов

Зачем компаниям вузы-партнеры?

Зачем вузам компании-партнеры?

02

positive education

Схема карьерных треков в кибербезе

Куда развиваться?

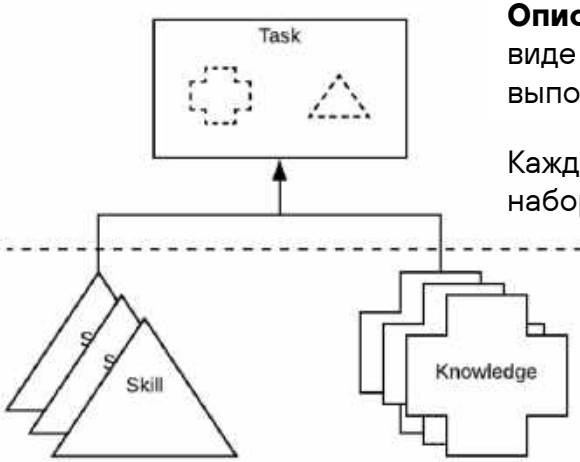
positive education

Доклад ЦСР «Северо-Запад» и Positive Technologies — это попытка определить возможный ландшафт рынка труда в информационной безопасности в 2027 году, а также предложить некоторую систему рекомендаций для участников рынка ИБ.

Читать отчет

Структура NICE (National Initiative for Cybersecurity Education) Framework

positive education

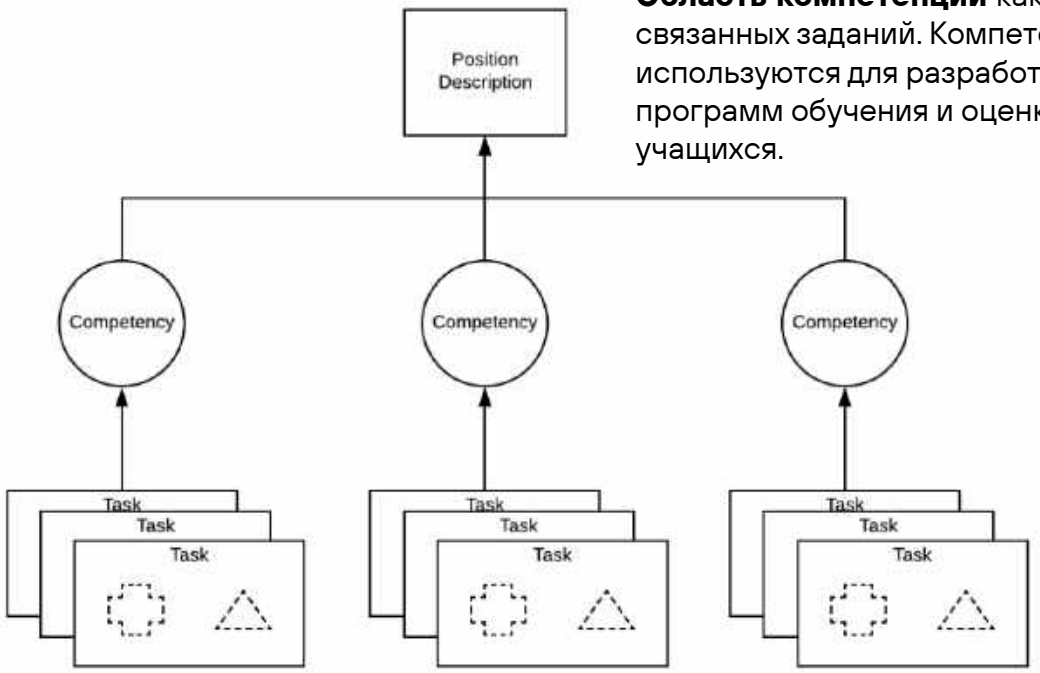


Описание работы в виде перечня выполняемых задач.

Каждая задача состоит из набор навыков и знаний.

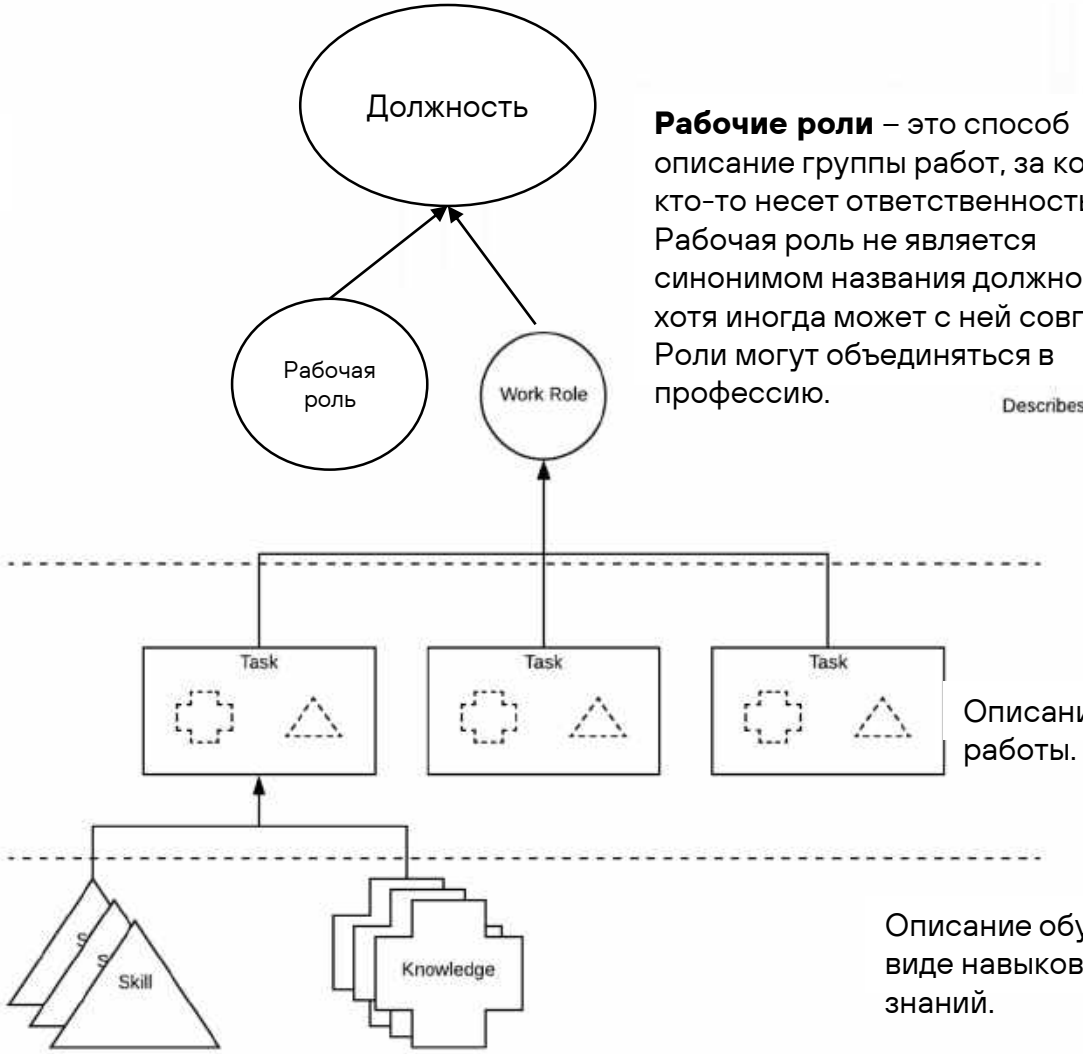
Описание обучения в виде навыков и знаний.

Рисунок 1



Область компетенций как группа связанных заданий. Компетенции используются для разработки программ обучения и оценки учащихся.

Рисунок 2



Рабочие роли – это способ описание группы работ, за которые кто-то несет ответственность. Рабочая роль не является синонимом названия должности, хотя иногда может с ней совпадать. Роли могут объединяться в профессию.

Описание работы.

Описание обучения в виде навыков и знаний.

Рисунок 3

Области деятельности в кибербезопасности

- Исследование безопасности
- Управление уязвимостями
- Администрирование средств защиты информации
- Центр противодействия киберугрозам (ЦПК) или SOC
- Комплаенс-аналитика
- Аналитика ИБ
- Безопасная разработка приложений

и др.

Не включаются:

- техническая защита информации
- криптография
- разработка СЗИ

Ролевая модель

positive education

PDF версия схемы

Читать о схеме

Смежные области знаний

Переходы между ролями

Энциклопедия ролей кибербезопасности

Почему роли, а не профессии?
Терминология в кибербезопасности
Обязательные знания и навыки в кибербезе
Примерные темы студенческих работ по кибербезу
Вузы по ИБ на карте
Роли 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
- Антифрод-аналитик
- Архитектор ИБ
- Специализация Безопасность Linux
- Специализация Безопасность Web3

Роли

Роли и специализации в кибербезопасности > Аналитик SOC L1

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;
- Составление рекомендаций для фильтрации ложных срабатываний сценариев выявления

Table of contents
- Обязанности
- Знания и навыки
- Дополнительно

Other Links
- СХЕМА карьерных т
результативной кибер
- Внести предложени
ролей с помощью GitH

positive education

Описание роли

Данная ролевая модель легла в основу Топ ИТ программы Минцифры по КБ

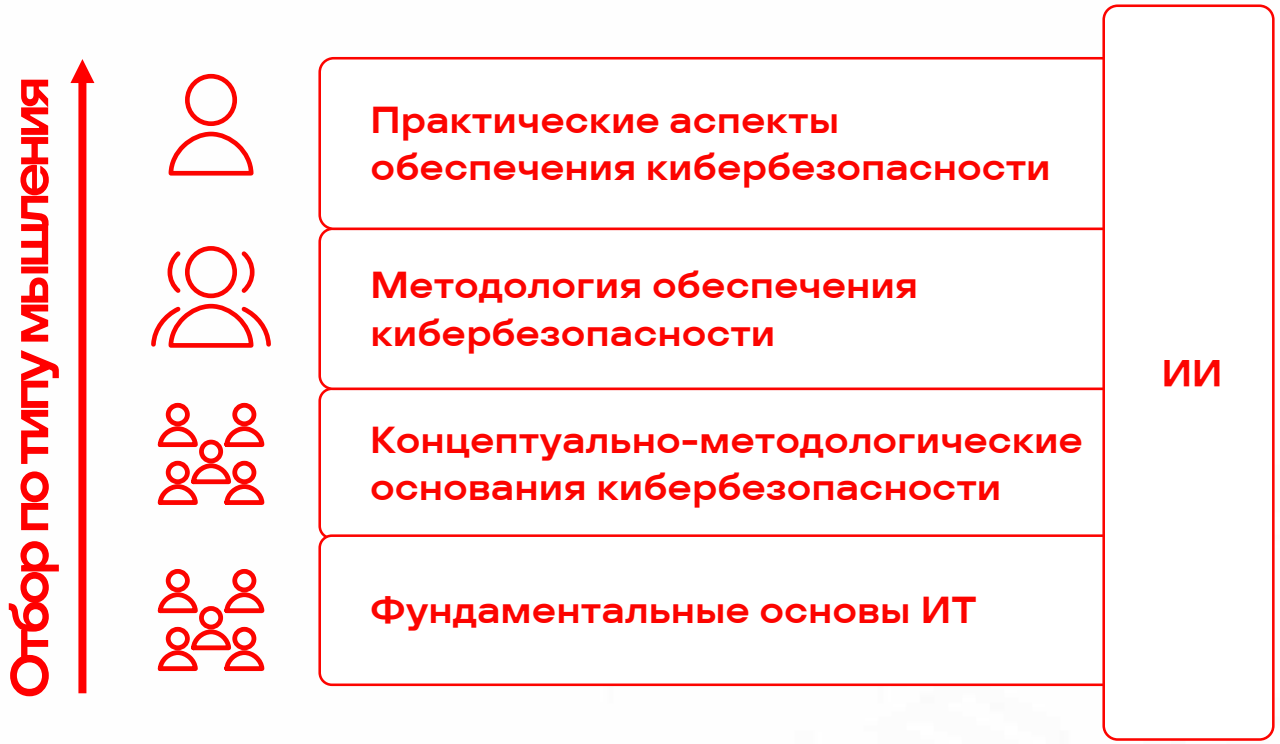
03

positive education

Кибербезопасность – специализация в ИТ

Чему учиться?

Кибербезопасность - специализация в ИТ



КБ требует особого типа мышления

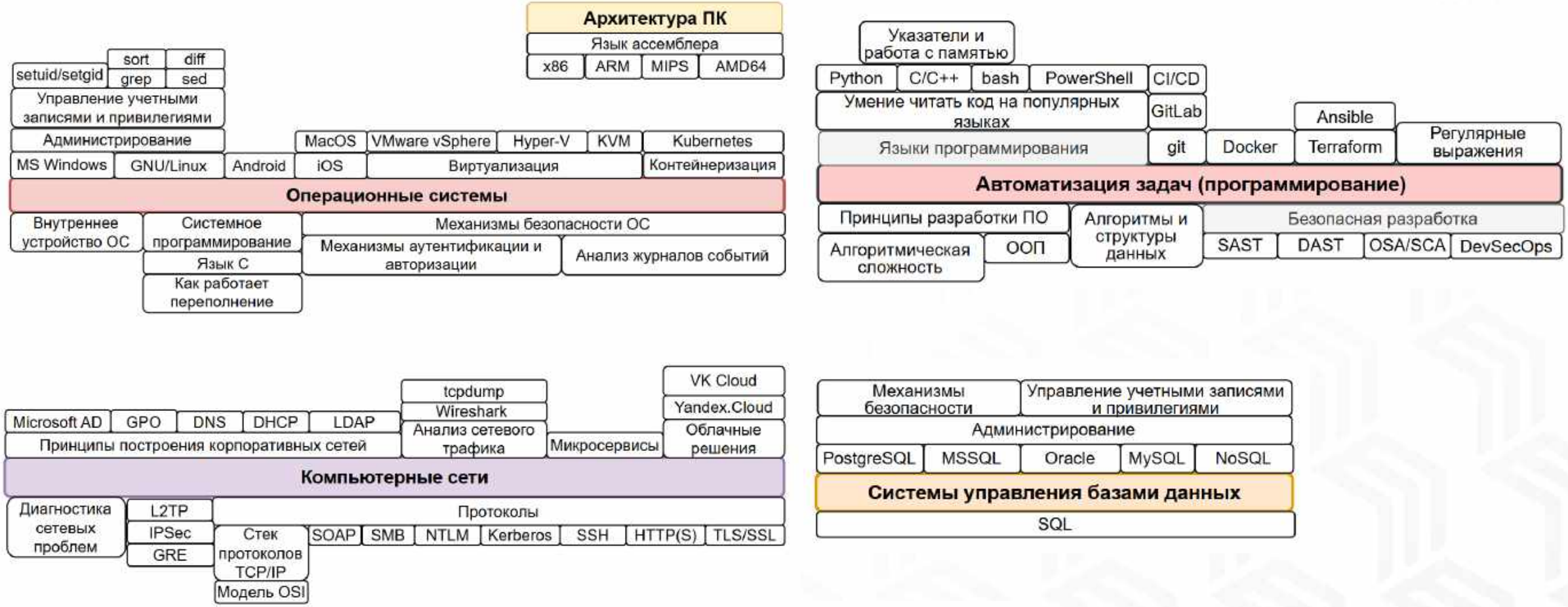
“**Такое мышление неестественно для большинства людей**. Оно неестественно для инженеров. Хорошая инженерия подразумевает размышления о том, как можно заставить систему работать; образ мышления в области безопасности подразумевает размышления о том, как можно заставить систему сломаться. Оно подразумевает 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)

Уровневая модель подготовки специалистов по обеспечению кибербезопасности

Кто это реализует?

Фундаментальные основы ИТ. Уровень 1



Учим ИТ-специалиста – формируем шаблоны из ИТ

Концептуально-методологические основания кибербезопасности. Уровни 2-3

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 информационной безопасности – антропные системы:
- человек (тело, психика, сознание)
- корпорация (активы, персонал, руководство)
- государство (инфраструктура, население, власть)

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

Концептуально-методологические основания кибербезопасности. Уровни 2-3

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

Объекты кибербезопасности – информационно-кибернетические системы

Кибербезопасность
ситуация, при которой киберсистемам и киберустройствам не может быть причинен существенный вред, с точки зрения их владельца:

- нарушения их работоспособности;
- перехвата управления;
- искажения/уничтожения обрабатываемых в них - информационных ресурсов;
- кражи информационных ресурсов с целью их противоправного использования.

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

Практические аспекты обеспечения кибербезопасности. Уровень 4

Учим КБ-специалиста – формируем шаблоны из КБ

04

positive education

Кибертренажер PT Education Technology Laboratory

edu.ptsecurity.com/pt_edtechlab

Нельзя научить – можно научиться

- Значения и смыслы не передаются от одного участника информационной коммуникации к другому. Передается текст. Значения и смыслы генерирует субъект, принимающий текст

- За рамками выступления остается проблема мотивации учащихся

Стек передачи информации

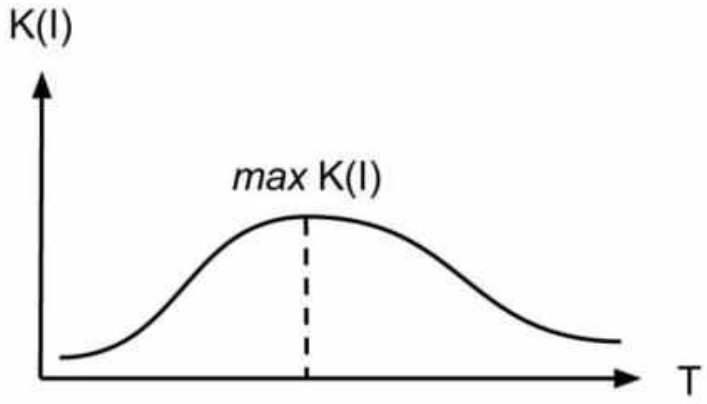
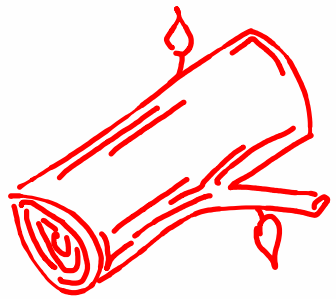


Рисунок 2 – График зависимости количества усвоенных знаний от объема тезауруса приемника

Источник:
Федоров, Д. Ю. Кибернетический подход к управлению процессом обучения на основе семантических сетей знаний [Текст] / Д.Ю. Федоров. – СПб. : Изд-во Политехн. ун-та, 2016. – 40 с.

Что такое результативное обучение кибербезопасности?



Философия

В основе обучения лежит философия результативного кибербеза

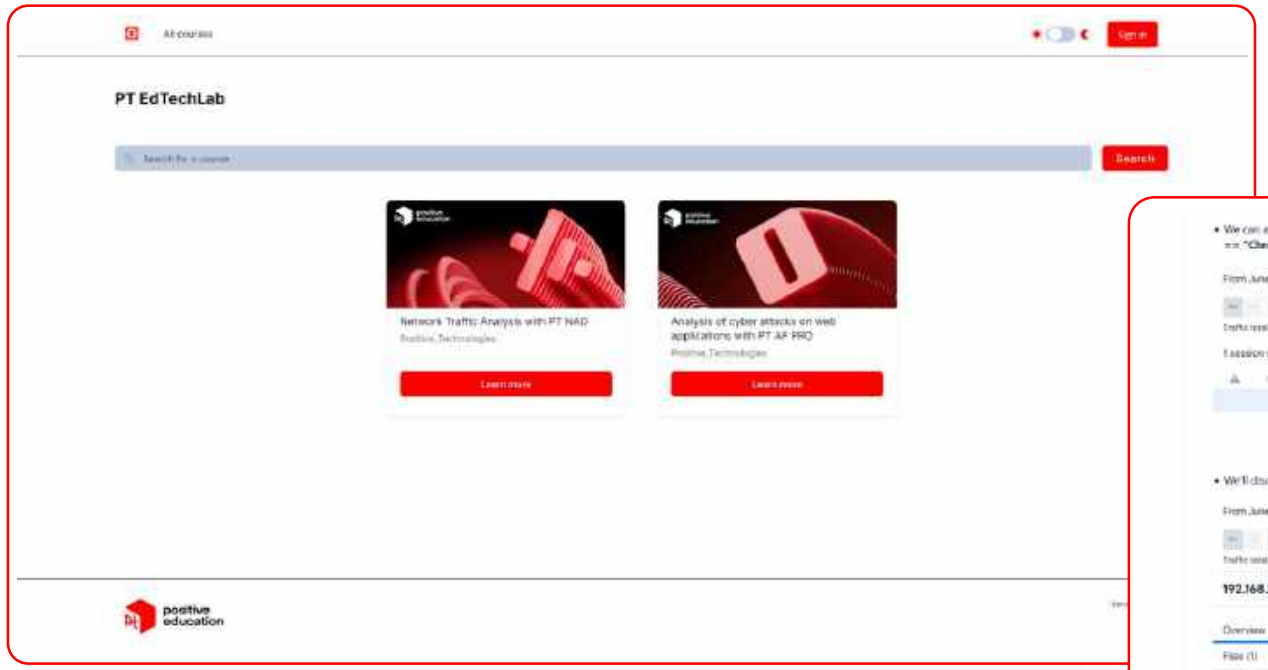
Практика

Практико-ориентированное обучение кибербезопасности на основе анализа реальных атак

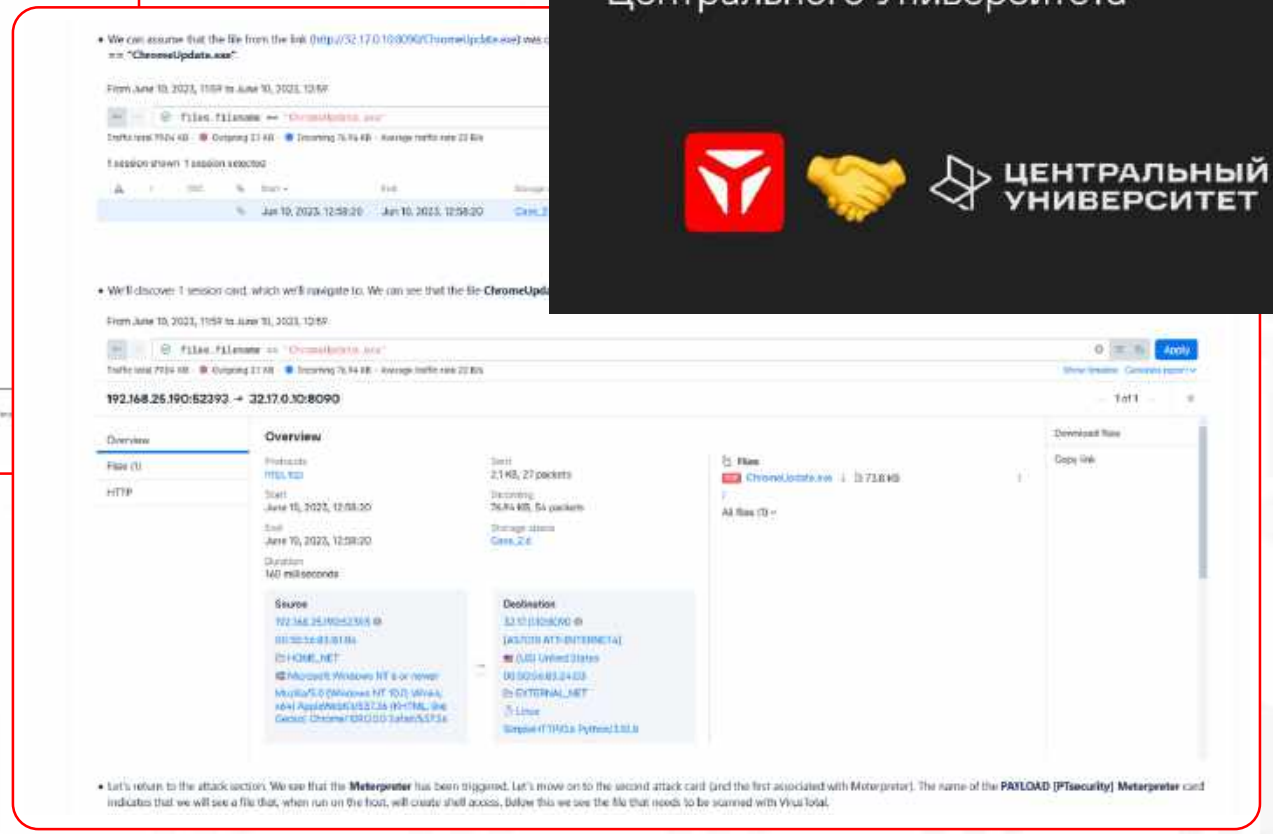
Ещё практика

Полученные навыки проверяются в боевых условиях на кибербитве

Как выглядит?



Стартовая страница



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

ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

Пример кейса

edu.ptsecurity.com/pt_edtechlab

Обучающие материалы, онлайн-курсы и сертификация по работе с СЗИ доступны для студентов и преподавателей вузов, ссузов.

positive education