ГУБКИНСКИЙ УНИВЕРСИТЕТ | ЗА ШАГ ДО СТОЛЕТИЯ!

С какими компетенциями надо выходить на рынок труда ИБ

Дмитрий Правиков
Заведующий кафедрой РГУ нефти и газа (НИУ) имени И. М. Губкина

Москва, 2025

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Итоги Всероссийской студенческой олимпиады по ИБ 2025

- **Восемь заданий – восемь компетенций**

ULYANOVSK STATE UNIVERSITY
УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

1890
КНИТУ

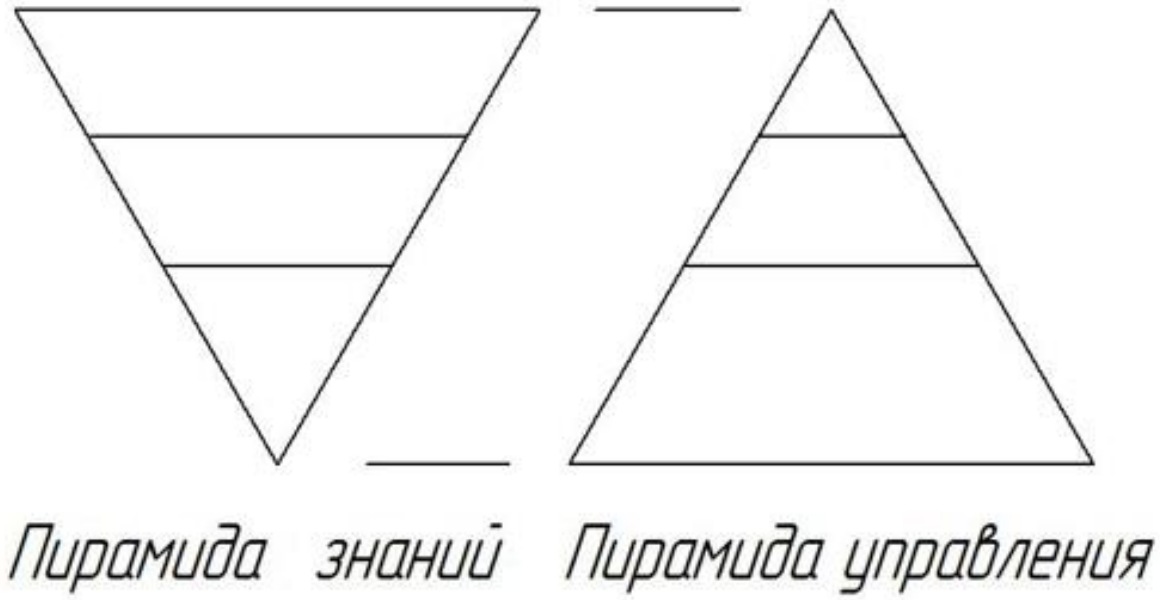
СГТУ
САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ГАГАРИНА Ю.А.

УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ

ПНИПУ

Что у нас сейчас на рынке труда?

Почему все хотят стать хакерами?



- Уровень безработицы менее 2,7%;
- Ужесточение ТК;
- Рост зарплат YoY 14,7%;
- Инфантилизация;
- Падение квалификации.

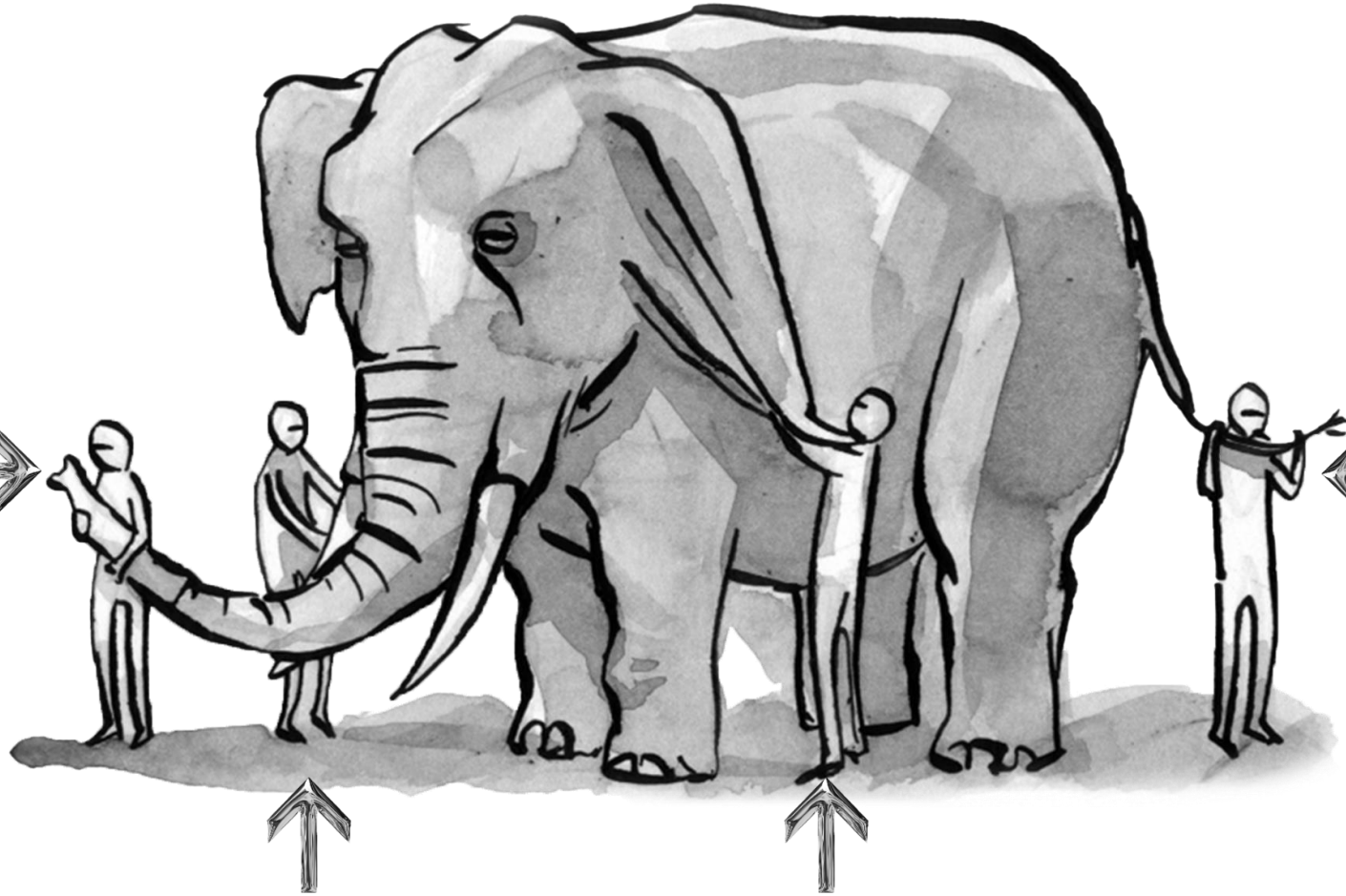
И. Ляпунов, генеральный директор Solar

«Рынок труда меняется стремительно. Но если раньше молодежь выходила на него с рюкзаком, амбициями и верой в себя, то теперь — с мамой, адвокатом, и трехтомником о границах личного комфорта»

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Проблема формирования компетенций

Каждый видит выпускника по-своему…



Регуляторы

Вендор

Высшая школа

Работодатель

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Формальное начало

А что делают на рынке информационной безопасности?

- **Общероссийский классификатор видов экономической деятельности (утв. Приказом Росстандарта от 31.01.2014 № 14-ст)**
- 74.90.9 Деятельность в области защиты информации и обеспечения безопасности критической информационной инфраструктуры:
- 74.90.91 Деятельность по разработке средств защиты информации
- 74.90.92 Деятельность по разработке информационных и телекоммуникационных систем, защищенных с использованием средств защиты информации
- 74.90.93 Деятельность по мониторингу информационной безопасности средств и систем информатизации
- 74.90.94 Деятельность по обеспечению защиты информации

Данные по анализу HH.RU (весна 2024 г.)

Инженер по информационной безопасности	**630 вакансий**
Специалист по информационной безопасности IT	**439 вакансий**
Специалист по сертификации средств защиты информации	**221 вакансия**
Системный инженер Linux	**200 вакансий**
Аналитик по информационной безопасности	**167 вакансий**

А. Петухов, Энерджинет НТИ

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Формирование специалиста по ИБ

•Концепция подготовки в Губкинском

Фундаментальная подготовка

В рамках учебной программы РГУ нефти и газа (НИУ) имени И. М. Губкина

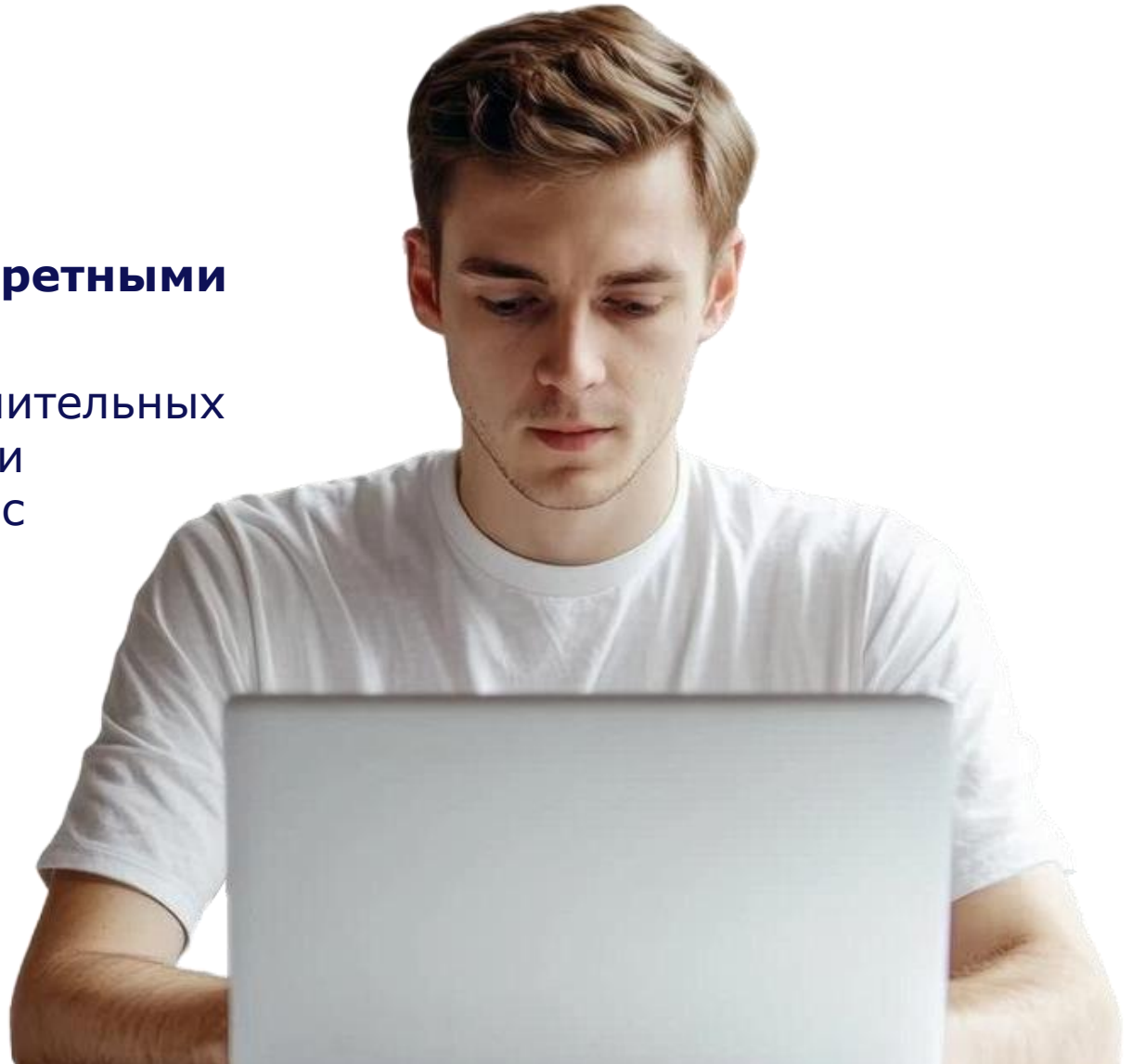
Практический опыт

Фактическое трудоустройство на старших курсах;

Прохождение практики на киберполигоне.

Владение конкретными СЗИ

В рамках дополнительных занятий по линии взаимодействия с вендорами



Выпускник специалитета 2025 года

Вендорская сертификация — это тренд

- ALTADM1. Курс Администрирование ОС Альт. Часть 1. ООО "Базальт СПО"
- ALTNET. Курс Интернет-службы в ОС Альт. ООО "Базальт СПО"
- ALTSHELL. Автоматизация (shell-скрипты) в ОС Альт. ООО "Базальт СПО"
- ALTSEC. Курс Информационная безопасность в ОС Альт. ООО "Базальт СПО"
- Certified Specialist (CS) по продукту PT NAD. Positive Technologies
- Ideco NGFW University
- Построение и защита сетей на базе продуктов UserGate
- Анализ трафика и защита сетей на базе продуктов UserGate
- Курс при поддержке Сбера в рамках совместной с ВМК МГУ им. М. В. Ломоносова магистерской программы "Кибербезопасность" — введение в информационную безопасность аппаратных решений

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Какая траектория лучше?

Мы вышли из «Болонского процесса»...

Бакалавриат:

Преимущество: 4 года обучения — сокращение времени для выхода на рынок труда

Недостаток: более узкий набор компетенций

Статистика: 77,4% трудоустроенных по специальности, средняя заработная плата х рублей

Специалитет:

Преимущество: более широкий набор компетенций

Недостаток: 5 или 5,5 лет обучения – увеличение времени для выхода на рынок труда;

Статистика: 100% трудоустроенных по специальности, средняя заработная плата 1,5х рублей.

По данным на 30 декабря 2024 года, подсистемы «Анализ трудоустройства граждан» Единой цифровой платформы в сфере занятости и трудовых отношений «Работа в России»

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Так какие же нужны компетенции?

Требования к специалистам центров мониторинга

Знать:

- Нормативные правовые акты, методические документы, национальные стандарты, нормативные акты регуляторов, устанавливающих требования по защите и мониторингу информационной безопасности объектов критической информационной инфраструктуры;
- Основные уязвимости и информационные угрозы, характерные для объектов критической информационной инфраструктуры;
- Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности;
- Основные тактики и техники атак (MITRE ATT&CK);
- Типовые сетевые атаки на инфраструктуру на различных уровнях модели OSI.
- Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости);
- Подходы к настройке средств сбора технических данных для выявления событий информационной безопасности;
- Принципы работы с техническими средствами, реализующими функции управления инцидентами информационной безопасности;
- Подходы к описанию сценариев реализации угроз информационной безопасности в субъектах критической информационной инфраструктуры;
- Подходы к реагированию на инциденты информационной безопасности в субъекте критической информационной инфраструктуры.

ГУБКИНСКИЙ УНИВЕРСИТЕТ

Так какие же нужны компетенции?

Требования к специалистам центров мониторинга

Уметь:

- Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации, международные и национальные стандарты в сфере информационной безопасности;
- Настраивать средства (агентов, интерфейсов) сбора технических данных для выявления событий информационной безопасности в значимых объектах критической информационной инфраструктуры;
- Осуществлять работу с техническими средствами, реализующими функции управления инцидентами защиты информации на значимых объектах критической информационной инфраструктуры;
- Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности на значимых объектах критической информационной инфраструктуры;
- Формировать отчетность о выявленных событиях и инцидентах информационной безопасности на значимых объектах критической информационной инфраструктуры.
- Работать с техническими средствами, реализующими функции управления инцидентами информационной безопасности;
- Применять меры, направленные на снижение тяжести последствий от реализации инцидентов информационной безопасности в субъекте критической информационной инфраструктуры;
- Применять методологию оценки потенциала влияния (критичности) инцидента информационной безопасности субъекта критической информационной инфраструктуры;
- Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности;
- Формировать отчетность в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после инцидентов информационной безопасности.

ГУБКИНСКИЙ УНИВЕРСИТЕТ | ЗА ШАГ ДО СТОЛЕТИЯ!

СПАСИБО ЗА ВНИМАНИЕ!

dip@gubkin.pro