РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ОЦЕНКА КОМПЕТЕНЦИЙ СТУДЕНТОВ В ОБЛАСТИ КРИПТОГРАФИИ ЧЕРЕЗ ПРИЗМУ РЕШЕНИЯ ЗАДАНИЙ ВСЕРОССИЙСКОЙ СТУДЕНЧЕСКОЙ ОЛИМПИАДЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

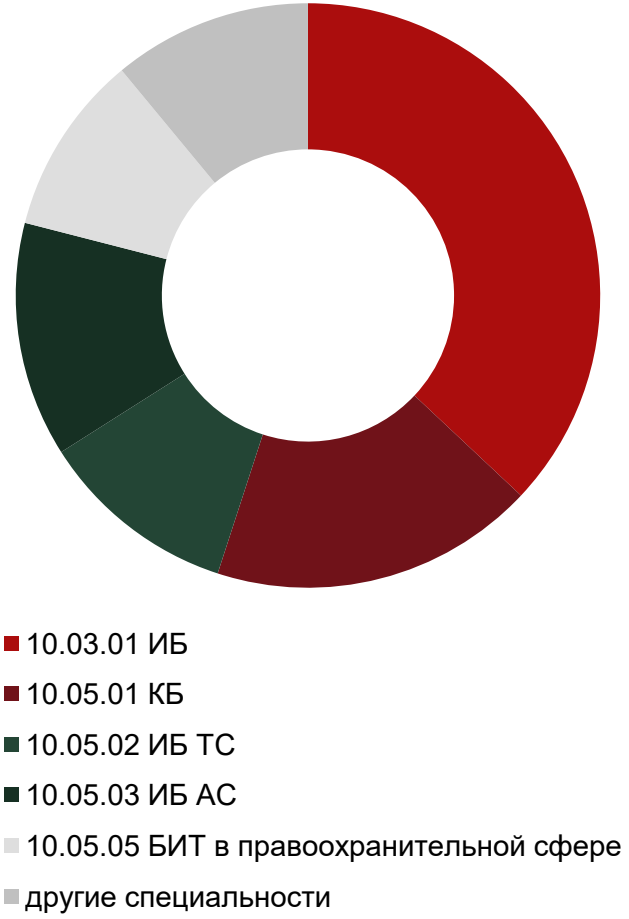
Д.И. Правиков, к.т.н., с.н.с., заведующий кафедрой комплексной безопасности критически важных объектов, РГУ нефти и газа (НИУ) имени И.М. Губкина
А.Б. Пичкур, к.ф-м.н., доцент, директор образовательных программ, Гарда Технологии

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ВСО ИБ)

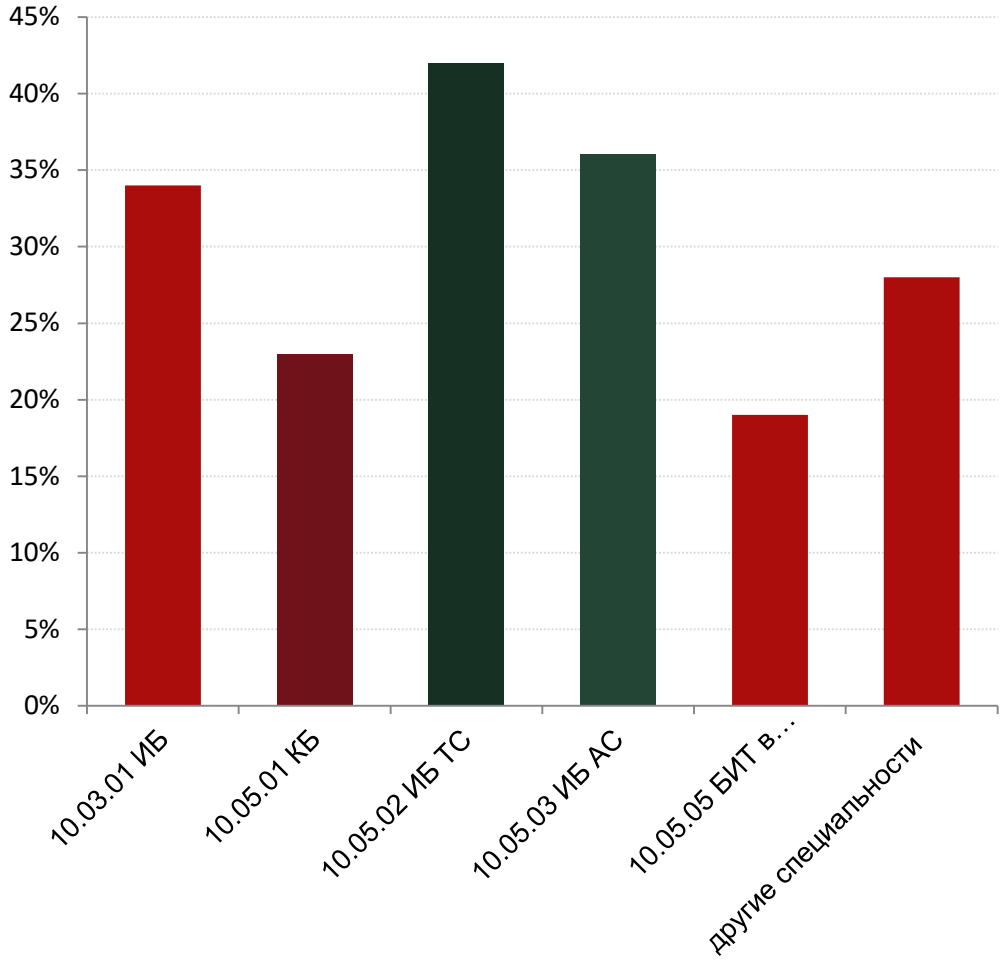
Проводится на базе Губкинского университета с 2022 года. Вопросы для отборочного (заочного), и финального (очного) этапов составляются ведущими компаниями, работающими в области ИБ и ИТ, в соответствии с компетенциями образовательных стандартов.

Анализ распределения участников отборочного (заочного) тура ВСО ИБ по специальностям (направлениям подготовки)

Участвовало 50+ вузов



Количество правильных решений блока заданий по криптографии отборочного тура ВСО ИБ по специальностям (направлениям подготовки)

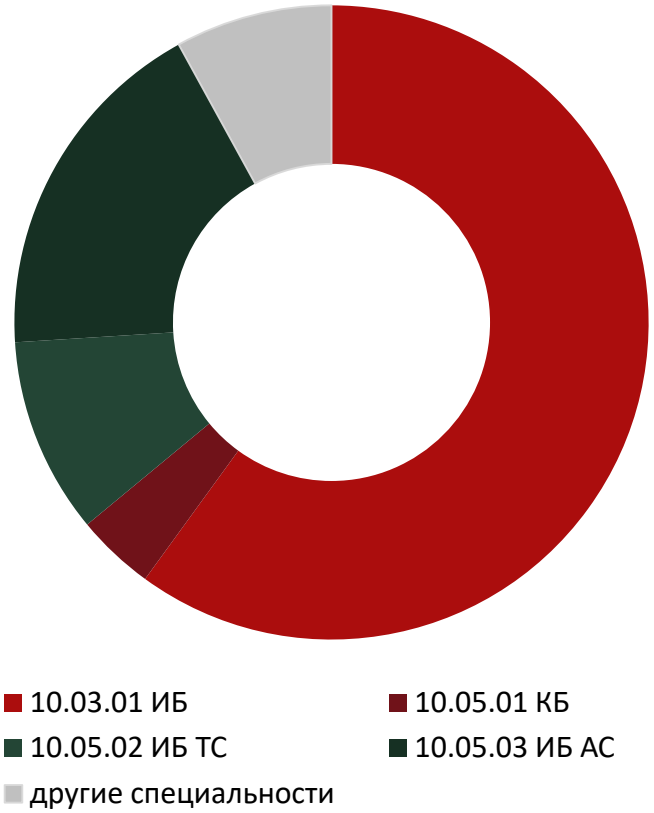


- Вопрос, связанный с криптосистемой Блюма-Гольдвассера, оказался трудным для участников. Ответом на задание был текст, полученный при расшифровании. Всего 8% участников правильно ответили на вопрос.

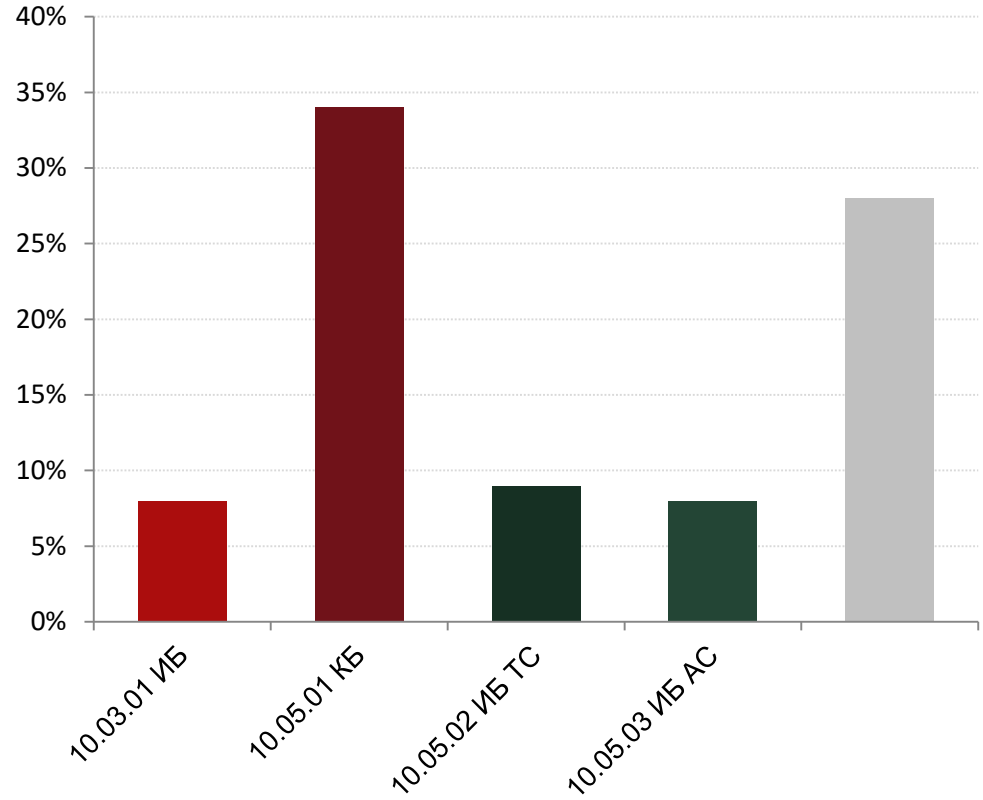
- По результатам анализа блока «Криптография», можем сделать вывод, что задания, связанные с математическими алгоритмами для обеспечения конфиденциальности, целостности и аутентичности информации, вызывают наибольшие трудности при решении у студентов.

Задачи по криптографии очного тура

- Блок состоял из 3 вопросов с общим условием: открыть папку, в которой есть шифрованный текст по условию задачи, ключ зашифрования, открытый текст и описан процесс зашифрования.
- С заданием, в котором требовалось проанализировав программу, восстановить алгоритм выработки гаммы и определить строение ключа, справились 17% участников.
- Сложнее оказался вопрос, где нужно было привести алгоритм нахождения ключа по шифрованному тексту, найти ключ и открытый текст. При этом участники олимпиады зачастую не применяли при решении данного задания такой универсальный метод, как перебор всех возможных ключей. Это говорит о недостаточном уровне математической подготовки и овладения основными криптографическими методами.

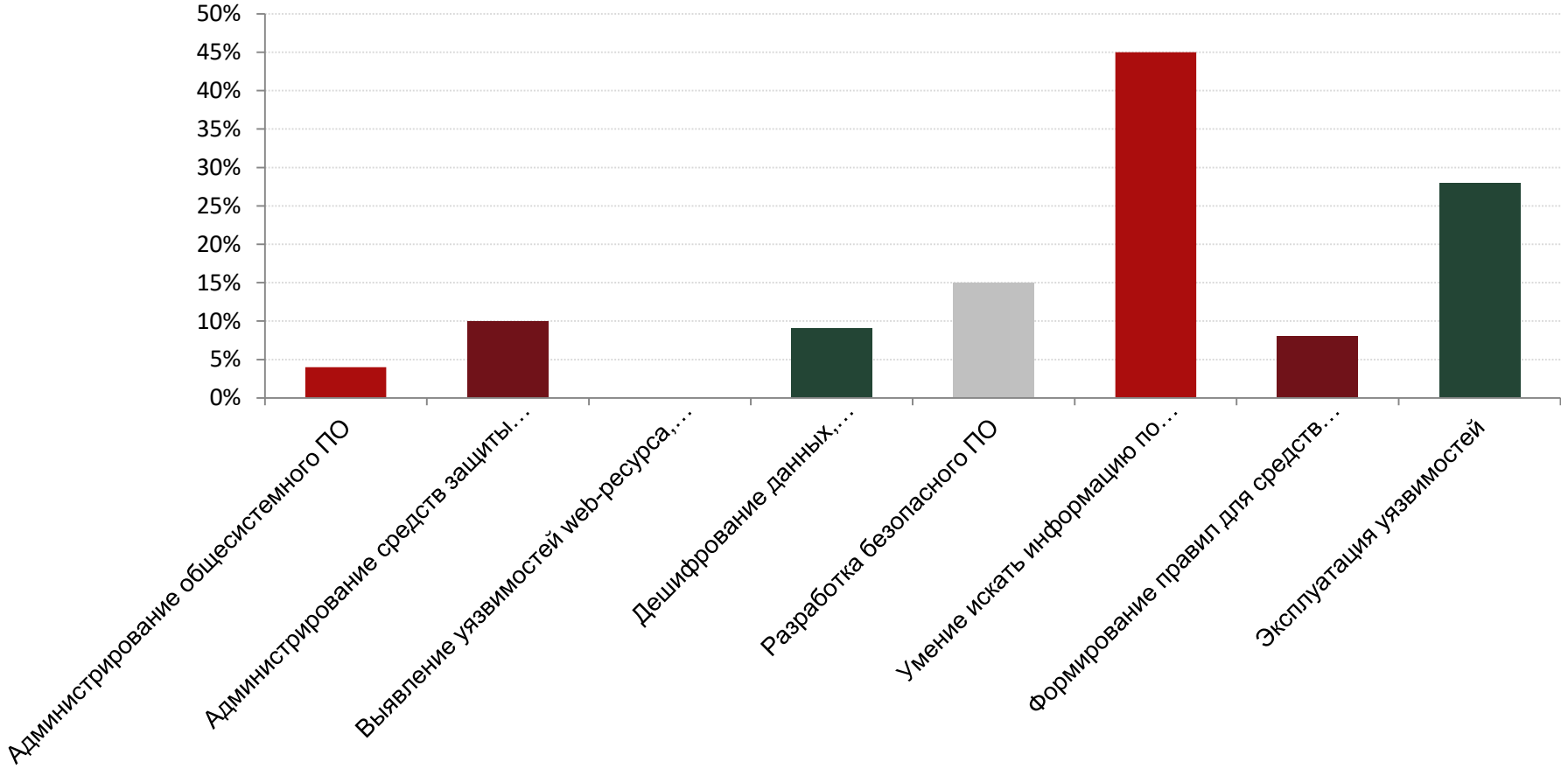


Распределение студентов по специальностям в очном туре



Распределение по специальностям правильных ответов по криптографическим задачам

Результаты
очного тура олимпиады по блокам заданий



ВЫВОДЫ

Проведенный анализ показал, что использование компетентностного подхода с привлечением ведущих компаний, работающих в сфере ИБ, для составления банка вопросов, для оценки соответствия компетенций будущих специалистов требованиям рынка труда, является допустимым.
Подводя итоги олимпиады, необходимо отметить, что студенты были оценены по восьми номинациям компаниями-партнерами. В номинации попали студенты разных специальностей, что свидетельствует о релевантности вопросов и корректности оценки компетенция участников. Задания олимпиады оказались подобраны таким образом, что отсутствует явный лидер, что говорит как о сбалансированности подхода, так и о невозможности «обнять необъятное» в рамках обучения.

Спасибо
за внимание!

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Д.И. Правиков, к.т.н., с.н.с., заведующий кафедрой комплексной безопасности критически важных объектов, РГУ нефти и газа (НИУ) имени И.М. Губкина, dip@gubkin.pro
А.Б. Пичкур, к.ф-м.н., доцент, директор образовательных программ, Гарда Технологии, a.pichkur@gardatech.ru