Саратовская олимпиада по криптографии 2020-2021 учебного года

Абросимов М.Б.[1], Салий В.Н.[2], Жаркова А.В.[3], Коннова А.Д.[4],
Лобов А.А.[5], Моденова О.В.[6], Шабаркова А.О.[7]
[1]*mic@rambler.ru*, [2]*saliivn@sgu.ru*, [3]*zharkovaav3@gmail.com*, [4]*konnova.anya2016@yandex.ru*,
[5]*aisanekai@mail.ru*, [6]*oginiel@rambler.ru*, [7]*shabarkova_alex.andra@mail.ru*
Саратовский государственный университет имени Н.Г. Чернышевского

В работе описывается история и эволюция Саратовских олимпиад по криптографии, которые с 2002 года проводятся кафедрой теоретических основ компьютерной безопасности и криптографии ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского. Подводятся итоги последней XIX открытой олимпиады школьников и студентов по криптографии, проведённой в 2020-2021 учебном году. Обсуждаются особенности подготовки и проведения соревновательных мероприятий в условиях ограничения возможности проведения очных мероприятий.

Ключевые слова: олимпиада школьников, олимпиада студентов, криптография, очные соревнования, дистанционные соревнования.

В 2002 году в Саратовском государственном университете имени Н.Г. Чернышевского была создана кафедра теоретических основ компьютерной безопасности и криптографии и открыта специальность «Компьютерная безопасность». Осенью-зимой 2002-2003 года была проведена первая олимпиада по криптографии. Олимпиада состояла из 4 туров и проводилась для старшеклассников в заочном формате. Задания каждого тура выкладывались на сайте [1] и рассылались по школам города Саратова. Каждый тур состоял из 5 задач, на решение которых отводилось 2 недели.

Задачи, которые предлагались участникам олимпиады, имели разную направленность. Среди задач, безусловно, встречались задачи, посвященные криптографии, в которых требовалось зашифровать, расшифровать или дешифровать какие-то сообщения по некоторым известным данным. Однако были и задачи математического направления, а также задания, связанные с информатикой или программированием. Чтобы успешно справиться с заданиями олимпиады, нужно было продемонстрировать хорошие знания и умения по математике, информатике и программированию, а также умение искать и привлекать дополнительную информацию, существенно выходящую за рамки школьной программы. Для решения задач можно было использовать любые доступные средства.

Решения участники присылали по электронной почте, после чего жюри выполняло проверку работ. Многие задания требовали развернутого решения. Все задачи олимпиады составлялись сотрудниками кафедры теоретических основ компьютерной безопасности и криптографии. В разные годы победителями олимпиады становились школьники из Саратова, Балакова, Хвалынска, Волгодонска, Рязани, Ярославля и других городов. Вне конкурса в олимпиаде принимали участие и студенты.

Основной целью проведения олимпиады было повышение интереса к криптографии и поощрение исследовательских навыков. Стоит отметить, что

большой сложностью проведения олимпиады в таком формате как для школьников, так и для организаторов была долгая продолжительность и отсутствие очного тура для выявления победителя в равных условиях.

С 2018 года олимпиада стала проводиться в два тура. Первый дистанционный тур (отборочный) стал проводиться в декабре. Продолжительность отборочного тура составляет одну неделю. Как правило, это первая полная неделя декабря – с понедельника по воскресенье. Задания публикуются на сайте кафедры, а для регистрации участников и ввода ответов используются возможности платформы Эрудит.Онлайн Научно-образовательного центра «Эрудит» [2]. По результатам отборочного тура все победители приглашаются на очный тур.

Второй тур (очный) проводится в январе на базе факультета компьютерных наук и информационных технологий Саратовского государственного университета. Количество задач первого и второго тура одинаково, однако, если на решение задач дистанционного тура даётся одна неделя, то на решение задач очного тура отводится только 3 часа. Некоторые задачи очного тура составляются с отсылкой к задачам дистанционного тура, что позволяет делать некоторые выводы о самостоятельности решения задач участниками.

В 2018-2019 годах участникам предлагалось по 10 задач.

С 2019 года олимпиада стала проводиться для трёх категорий участников:

– ученикам 6-8 классов предлагается 6 задач;
– ученикам 9-11 классов – 8 задач;
– студентам – 10 задач.

С 2018 года задания стали проверяться в полуавтоматическом режиме. Сначала задания проверяются автоматически с помощью программного обеспечения платформы Эрудит.Онлайн. Далее задания проверяются членами жюри в ручном режиме. В силу особенности олимпиады большинство задач составляется так, чтобы ответом было некоторое сообщение. Задачи могут иметь несколько решений, в том числе и не предусмотренных заранее авторами заданий. Хотя процент таких решений чрезвычайно низок, для выявления таких решений и используется ручная проверка. Так, например, одна из задач формулировалась следующим образом:

Назовите слово из четырех букв, которое будет существительным, если поставить ударение на букву, стоящую в русском алфавите десятой, и глаголом, если поставить ударение на букву, которая стоит в алфавите первой. Ответ запишите заглавными буквами.

Решением жюри было слово **ЖИЛА**. Большинство участников, которые дали ответ на эту задачи, указали именно это слово. Однако один из участников нашёл и другое решение – **ЛИЛА**. Как оказалось, с ударением на первый слог это название индийской настольной игры. Таким образом, верные решения, которые не были предусмотрены авторами задач и членами жюри, при автоматической проверке оцениваются как ошибочные, однако на втором этапе,

при ручной проверке, ответ оценивается как верный и участники получают полные баллы.

В новом формате по-прежнему предлагаются задания не только по криптографии, и для успешного решения могут потребоваться знания по информатике, программированию и математике. Многие задачи допускают различные решения: можно составить программу, а можно найти математическое решение.

Особенностью олимпиады по криптографии является то, что разрешается использовать все доступные средства: любые системы программирования, собственные или сторонние программы, справочные материалы, сеть Интернет. Обязательным условием является лишь индивидуальное участие. На дистанционном туре проверить это практически невозможно, однако на очном туре запрещается использовать мессенджеры и иные средства общения. Для решения задач, связанных с криптографией, желательно знакомство с классическими шифрами, которое можно получить из книг, вполне доступных школьникам [3]. Задания олимпиад за все годы представлены на сайте [1].

В 2020-2021 учебном году проведение очного тура представлялось практически невозможным из-за эпидемиологических ограничений. Дистанционный тур проводился с 7 по 13 декабря 2020 года. В отборочном туре приняли участие 244 участников: 70 учеников 6-8 классов, 108 учеников 9-11 классов и 66 студентов. Среди участников были школьники и студенты из России, Республики Беларусь и Республики Молдова. По результатам первого тура победители получили приглашение на второй очный тур, который состоялся 31 января.

В условиях сложной эпидемиологической обстановки было принято решение очный тур провести в режиме онлайн на базе платформы ZOOM. Во II туре приняли участие 28 участников из городов Абакан, Саратов, Ершов, Путилково (Россия) и города Рыбница (Республика Молдова). Соблюдение регламента олимпиады контролировали сотрудники лаборатории компьютерной безопасности, что позволило считать, что все участники находятся в равных условиях и решают задания олимпиады самостоятельно. Положительным моментом такого способа проведения олимпиады стала возможность существенного увеличения географии участников очного тура: впервые в очном туре Саратовских олимпиад по криптографии приняли участие школьники из других городов России и даже из других стран – школьники из Республики Молдовы стали призёрами олимпиады, заняв 2 место.

Список литературы

[1] Олимпиады по криптографии. URL: https://www.sgu.ru/structure/computersciences/theorcompsafe/olimpiady-po-kriptografii

[2] Портал дистанционных конкурсов и олимпиад Эрудит.Онлайн. URL: https://erudit-online.ru

[3] *Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: «Гелиос АРВ», 2002.