Информация
по представлению проектных работ на всероссийскую олимпиаду школьников по информатике (профиль – Информационная безопасность)

Представление и защита проекта является обязательным условием участия в региональном этапе олимпиады. Электронные варианты проектов необходимо предоставить **до 15 января 2026 г.** включительно.

Для презентации проекта в очной форме на каждого участника выделяется от 5 до 10 минут.

На региональный этап допускается предоставление проекта со степенью готовности порядка 75% при условии прозрачного и аргументированного описания всех недоработанных частей в пояснительной записке.

Для защиты участник предоставляет:

– проектный продукт (например, программный код, прототип системы, методику проведения тестов);

– пояснительную записку, оформленную в соответствии с ГОСТ 7.32-2017, которая является развернутым описанием всей деятельности учащегося при выполнении проекта;

– презентацию для выступления на защите.

Пояснительная записка в формате PDF. Название документа ПЗ – ФИО в именительном падеже – название творческого проекта.

Презентация (название документа ПЗ – ФИО в именительном падеже – название творческого проекта), подготовленная к защите должна иметь титульный лист аналогичный титульному листу пояснительной записки проекта, в том числе с указанием ФИО и должности руководителя участника проекта. Презентация выполняется с использованием компьютерных программ художественной графики, например, Power Point. Презентация должна содержать не менее 10 слайдов и отражать основные этапы и результаты исследования.

Для выполнения проекта участник должен выбрать одно из двух направлений для своего проекта: Red Team или Blue Team. Выбор направления определяет цели, методы и конечный продукт проекта.

Red Team - это подход к оценке безопасности, при котором участник моделирует тактики, техники и процедуры (TTP) реального злоумышленника с целью проверки устойчивости систем, процессов и персонала к целенаправленной атаке. В контексте проекта данное направление нацелено на проактивный поиск, исследование, доказательство и демонстрацию уязвимостей и слабых мест в информационных системах, программном обеспечении или организационных процессах.

Blue Team - это подход, нацеленный на создание, внедрение и поддержание эффективных контрмер для защиты информационных активов от киберугроз. В рамках проекта участник выступает в роли защитника, чья задача - разработать решение, которое повышает общий уровень безопасности системы, упрощает работу аналитиков или автоматизирует рутинные операции по обеспечению ИБ (например,

прототип системы обнаружения вторжений (IDS) или предотвращения вторжений (IPS); инструмент для мониторинга и анализа логов безопасности; средство для контроля настроек безопасности операционных систем или приложений.

В рамках выбранного направления участнику предлагается самостоятельно на основе открытых источников выявить и конкретизировать произвольную, но существующую и подтверждённую определённым кругом источников проблему информационной безопасности. Это может быть, например, слабость популярных средств обеспечения информационной безопасности, типичная проблема использования информационных систем, отсутствие инструмента защиты от известной угрозы информационной безопасности или иная подобная проблема. Далее участнику предстоит сформулировать задачу решения конкретизированной проблемы любым доступным ему способом (алгоритмически, программно, программно-аппаратно, построением математического метода или иначе) и в рамках выполнения проекта реализовать предложенное решение.

Требования к оформлению проекта:

- текст проекта предоставляется в электронном виде, в текстовом формате (*.doc, *.docx, *.rtf) на русском языке;

- объём проекта – не менее 10 и не более 20 с. (без приложений)

Электронный вариант проекта высылается на электронную почту kit@dgunh.ru Бумажный вариант высылается по адресу – г. Махачкала, ул. Джамалутдина Атаева, д.5, ГАОУ ВО «Дагестанский государственный университет народного хозяйства», кафедра «Информационные технологии и информационная безопасность».