Уважаемый участник олимпиады!

17 и 19 января 2026 года пройдёт региональный этап всероссийской олимпиады школьников по информатике, профиль «Информационная безопасность».

Место проведения: МАОУ лицей № 180 «Полифорум», г. Екатеринбург, ул. Крестинского, 53а.

Программа олимпиады будет размещена на сайте Фонда «Золотое сечение» https://zsfond.ru/vsosh/regionalnyj-etap/informatika-regionalnyj-etap/ не позднее 26 декабря 2025 года.

Олимпиада включает в себя два тура:

- практический тур (проводится 17 января для всех участников, продолжительность тура - 5 часов);
- проектный тур (проводится 19 января для всех участников в формате постерной сессии).

Общая оценка регионального этапа: 70% практический тур, 30% проектный тур.

Регламент и требования к проведению олимпиады определены в Требованиях Центральной предметно-методической комиссии по информатике, опубликованных на сайте Фонда «Золотое сечение» https://zsfond.ru/wp-content/uploads/2025/11/trebovaniya-k-re-vsosh-2025-26.pdf (с. 103-119)

На проектный тур участники олимпиады готовят проект, который представляет собой самостоятельную исследовательскую и опытно- конструкторскую работу участника, выполняемую в соответствии с утверждённым техническим заданием (ТЗ). ТЗ должно содержать чётко определённые требования к функционалу, результатам и критерии оценки итогового проектного продукта.

На региональный этап допускается предоставление проекта со степенью готовности порядка 75% при условии прозрачного и аргументированного описания всех недоработанных частей в пояснительной записке. Допускаются незначительные отклонения от первоначального ТЗ, которые должны быть обоснованы в документации.

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

Направление «Red Team»

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.

Примеры:

- инструмент для автоматизации сканирования уязвимостей или эксплуатации известных слабостей;
- исследование и описание нового вектора атаки на определенную информационную систему или технологию;
- методика проведения пентеста для конкретного класса систем (веб-приложений, сетевой инфраструктуры и т.д.).

Направление «Blue Team»

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

Примеры:

- 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, ведущая к нарушению конфиденциальности, целостности или доступности данных; отсутствие инструмента защиты от известной угрозы; новый класс уязвимостей или атак.

Критерии оценки проекта в Приложении1.

На проектный тур участник предоставляет:

– пояснительную записку, оформленную в соответствии с ГОСТ 7.32-2017, которая является развернутым описанием всей деятельности учащегося при выполнении проекта;
– проектный продукт (например, программный код, прототип системы, методику проведения тестов);
– постер или презентацию для выступления на защите.

Пояснительные записки необходимо направить в срок **до 12 января** на электронную почту **olymp-proect@zsfond.ru.** В теме письма указать – «Проект по информатике, профиль Информационная безопасность».

Оценка проектного тура:

– пояснительная записка – 10 баллов;
– оценка разработанного продукта – 10 баллов;
– оценка защиты проекта – 10 баллов.

Защита проекта:

– защита проходит в устном формате в виде постерной сессии;
– участник представляет плакат (постер) или презентацию (не более 5 содержательных слайдов), на которых отображены актуальность проекта, ход и результат его выполнения;
– члены жюри обходят участников постерной сессии и задают вопросы;
– члены жюри могут задавать вопросы участнику в течение 15 минут;
– по решению жюри защита может быть проведена в режиме последовательного выступления участников с демонстрацией постеров или презентаций.

Апелляция к результатам проектного тура не предусмотрена!

Практический тур.

Тематика заданий практического тура

1. Reverse/PWN – реверс-инжиниринг (анализ исходных текстов компьютерных программ).
2. Web – поиск уязвимостей веб-приложений.
3. Forensic – поиск следов инцидентов информационной безопасности.
4. Privesc/Misc – Linux\Unix (Misc) – задания смешанной категории, защита ОС Linux\Unix.
5. Crypto – криптография.
6. СЗИ – средства защиты информации.

Большая часть заданий имеет 2 флага – принцип: «1 задача – несколько вопросов». В ходе решения конкретного инцидента безопасности нужно получить сначала «лёгкий» (1-2 балла), потом «сложный» флаг (более 2 баллов).

Успешно найденный флаг для большинства заданий имеет формат vsosh{…} в любом регистре. Иное оговаривается в задании отдельно. Например, «*флаг необходимо сдать в формате: vsosh{команду, которую код выполняет скрытно от оператора}, т.е. ответ*

обернуть в форму vsosh{}».

На виртуальной машине участника установлен Kali Linux. Дополнительно установлены утилиты:

Ghidra, IDA Freeware 9.2, gdb с расширениями pwndbg и gef, edb, strace, ltrace, dirsearch, go, curl, LibreOffice, binwalk. Дополнительно установлены модули Python 3: pwntools, pybase64, sympy, pycryptodome и расширение BurpSuite: JWT Editor.

Volatility folder:
/home/kali/volatility-2.6.1
/home/kali/volatility3

Все инструкции будут размещены на рабочих столах виртуальных машин.

С примерами заданий прошлых лет можно ознакомиться на странице https://vsosh.miem.hse.ru/

Ресурсы для подготовки к практическому туру:

Базовый курс по CTF https://stepik.org/course/132488/promo

Курс молодого бойца CTF https://kmb.cybber.ru/

Обучение кибербезопасности https://picoctf.org/

Курс по ИБ для школьников https://course.ugractf.ru/

Архив квестов и решений из разных игр CTF https://freehackquest.com/

Подготовка к CTF https://codeby.net/threads/kak-podgotovit-sya-k-svoyemu-pervomu-ctf-poshagovyi-plan-dlya-novichkov.85833/

Стеганография https://codeby.net/threads/polnoye-rukovodstvo-po-steganografii-dlya-ctf-instrumenty-i-metody-poiska-skrytykh-dannykh.84884/

О CTF https://startx.team/blog/statyi/capture-the-flag-v-kiberbezopasnosti/
https://vk.com/@spbctf-ctf-for-beginners

Бесплатный курс по веб-безопасности https://portswigger.net/web-security

Задания для решения https://portswigger.net/web-security/all-labs

Платформа с большим количеством задач https://forkbomb.ru/

Тренировочные задания https://hackerlab.pro/training

Симулятор CTF https://www.hackthebox.com/

Форум информационной безопасности https://codeby.net/

Приложение 1

Критерии оценивания проектного тура (Направление «Red Team»)

Критерии оценки проекта			**Баллы**
Пояснительная записка 10 баллов	**1**	**Содержание и оформление документации проекта**	**10**
	1.1	**Общее оформление: (ориентация на ГОСТ 7.32-2001 Международный стандарт оформления проектной документации)**	**5**
	1.1.1	Соответствие ГОСТ 7.32-2017 (полное – 1, частичное – 0.5, нет – 0)	1
	1.1.2	Полнота и структурированность описания этапов выполнения проекта (полное – 2, частичное – 1, нет – 0)	2
	1.1.3	Глубина анализа предметной области и аналогов (глубокий – 1, поверхностный – 0.5, нет – 0)	1
	1.1.4	Качество и оформление списка литературы и источников (соответствует стандарту – 1, не соответствует стандарту – 0)	1
	1.2	**Качество теоретического и практического исследования**	**5**
	1.2.1	Актуальность и обоснование выбранной уязвимости/вектора атаки (да – 1, нет – 0)	1
	1.2.2	Четкость формулировки цели, задач и гипотезы (полное – 1, частичное – 0.5, нет – 0)	1
	1.2.3	Новизна предложенного метода атаки или инструмента (высокая – 1, средняя – 0.5, нет – 0)	1
	1.2.4	Описание методологии разработки и тестирования средства (детальное – 1, поверхностное – 0.5, нет – 0)	1
	1.2.5	Глубина анализа результатов тестирования и эффективности защиты (глубокий – 1, поверхностный – 0.5, нет – 0)	1
Оценка разработанного продукта 10 баллов	**2**	**Оценка продукта**	**10**
	2.1	**Функциональность и технологичность**	**6**
	2.1.1	Глубина проработки атаки: Продукт демонстрирует эксплуатацию уязвимости на уровне кода/логики/протокола, а не поверхностное сканирование (глубокая – 2, средняя – 1, низкая – 0.5)	2
	2.1.2	Масштаб охвата угроз: Разработка направлена на выявление и демонстрацию не единичной уязвимости, а класса уязвимостей или тактики атаки (класс уязвимостей – 2, тактика – 1, единичная уязвимость – 0.5)	2
	2.1.3	Степень автоматизации и воспроизводимости: Инструмент автоматизирует процесс атаки от разведки до получения результата, обеспечивая стабильное воспроизведение (полная – 2, частичная – 1, отсутствует – 0)	2
	2.2	**Качество исполнения и новизна**	**4**
	2.2.1	Архитектура и дизайн (читаемость, модульность) (высокие – 1, средние – 0.5, низкие – 0)	1
	2.2.2	**Новизна вектора атаки или подхода:** Предложен ранее не описанный метод эксплуатации или существенно доработан существующий (новый – 1, доработка – 0.5, стандартный – 0)	1

Критерии оценки проекта			Баллы
	2.2.3	**Практическая ценность для защиты:** Результаты работы продукта позволяют сформулировать конкретные рекомендации по усилению защиты для целого класса систем (высокоя – 1, средняя – 0.5, низкая – 0)	2
Оценка защиты проекта 10 баллов	**3**	**Процедура презентации проекта**	**10**
	3.1	**Качество презентации и процедуры защиты**	**6**
	3.1.1	Структура и логика изложения (четкая – 2, частичная – 1, отсутствует – 0)	2
	3.1.2	Качество подачи материала (ясность, убедительность, использование визуализации) (высокое – 2, среднее – 1, низкое – 0.5)	2
	3.1.3	Соблюдение регламента выступления (да – 1, нет – 0)	1
	3.1.4	Наглядность и успешность демонстрации продукта (полная – 1, частичная – 0.5, нет – 0)	1
	3.2	**Глубина понимания и ответы на вопросы**	**4**
	3.2.1	Понимание принципов защиты, моделей угроз (например, MITRE ATT&CK) (глубокое – 2, поверхностное – 1, нет – 0)	2
	3.2.2	Качество аргументации выводов, ограничений и путей развития системы (высокое – 1, среднее – 0.5, низкое – 0)	1
	3.2.3	Уверенность и аргументированность ответов на вопросы (высокие – 1, средние – 0.5, низкие – 0)	1
		Итого	**30**

Критерии оценивания проектного тура (Направление «Blue Team»)

Критерии оценки проекта			Баллы
Пояснительная записка 10 баллов	**1**	**Содержание и оформление документации проекта**	**10**
	1.1	Общее оформление: (ориентация на ГОСТ 7.32-2001 Международный стандарт оформления проектной документации)	5
	1.1.1	Соответствие ГОСТ 7.32-2017 (полное – 1, частичное – 0.5, нет – 0)	1
	1.1.2	Полнота и структурированность описания этапов выполнения проекта (полное – 2, частичное – 1, нет – 0)	2
	1.1.3	Глубина анализа предметной области и аналогов (глубокий – 1, поверхностный – 0.5, нет – 0)	1
	1.1.4	Качество и оформление списка литературы и источников (соответствует стандарту – 1, не соответствует стандарту – 0)	1
	1.2	**Качество теоретического и практического исследования**	**5**
	1.2.1	Актуальность и обоснование выбранной угрозы и средства защиты	1
	1.2.2	Четкость формулировки цели, задач и модели угроз (полные – 1, частичные – 0.5, нет – 0)	1
	1.2.3	Новизна предложенного метода защиты или анализа (высокая – 1, средняя – 0.5, нет – 0)	1
	1.2.4	Описание методологии тестирования (детальное – 1, поверхностное – 0.5, нет – 0)	1
	1.2.5	Глубина анализа полученных результатов и выводов (глубокий – 1, поверхностный – 0.5, нет – 0)	1
	2	**Оценка продукта**	**10**

Критерии оценки проекта			Баллы
Оценка разработанного продукта 10 баллов	**2.1**	**Функциональность и технологичность**	**6**
	2.1.1	**Уровень повышения защищенности:** Внедрение продукта значительно повышает устойчивость системы к целевому классу угроз (значительное – 2, среднее – 1, незначительное – 0.5)	2
	2.1.2	Широта охвата контрмер: продукт обеспечивает защиту от единичной уязвимости – 0.5, от тактики злоумышленника (по MITRE ATT&CK) – 1, от нескольких тактик или всей цепочки кибератаки – 2	2
	2.1.3	Эффективность продукта (высокая – 2, средняя – 1, нет – 0)	2
	2.2	**Качество исполнения и новизна**	**4**
	2.2.1	Проактивность и адаптивность: Решение способно не только детектировать известные угрозы, но и адаптироваться к новым или применять проактивные методы защиты (да – 1, частично – 0.5, нет – 0)	2
	2.2.2	Масштабируемость и модульность архитектуры: Архитектура продукта позволяет расширять его функциональность и применять в различных конфигурациях (продумана – 1, базово – 0.5, отсутствует – 0)	2
Оценка защиты проекта 10 баллов	**3**	**Процедура презентации проекта**	**10**
	3.1	**Качество презентации и процедуры защиты**	**6**
	3.1.1	Структура и логика изложения (четкая – 2, частичная – 1, отсутствует – 0)	2
	3.1.2	Качество подачи материала (ясность, убедительность, использование визуализации) (высокое – 2, среднее – 1, низкое – 0.5)	2
	3.1.3	Соблюдение регламента выступления (да – 1, нет – 0)	1
	3.1.4	Наглядность и успешность демонстрации продукта (полная – 1, частичная – 0.5, нет – 0)	1
	3.2	**Глубина понимания и ответы на вопросы**	**4**
	3.2.1	Понимание тактик, техник и процедур (TTP) в контексте проекта (глубокое – 2, поверхностное – 1, нет – 0)	2
	3.2.2	Качество аргументации выводов и предложенных контрмер (высокое – 1, среднее – 0.5, низкое – 0)	1
	3.2.3	Уверенность и аргументированность ответов на вопросы (высокие – 1, средние – 0.5, низкие – 0)	1
		Итого	**30**