ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РЕГИОНАЛЬНОГО ЭТАПА ВСЕРОССИЙСКОЙ ОЛИМПИАДЫ ШКОЛЬНИКОВ В 2025/26 УЧЕБНОМ ГОДУ

Москва, 2025

2.5.4. Профиль «Информационная безопасность»

1. Общие положения

1.1. Настоящие требования к проведению регионального этапа всероссийской олимпиады школьников по информатике профиля “Информационная безопасность” составлены в соответствии с Порядком проведения всероссийской олимпиады школьников, утвержденным приказом Министерства просвещения Российской Федерации от 27 ноября 2020 г. № 678 «Об утверждении Порядка проведения всероссийской олимпиады школьников».

1.2. Консультации по вопросам организации и проведения регионального этапа всероссийской олимпиады школьников по информатике можно получить по электронной почте, обратившись по адресу **vos-ib@miem.hse.ru** в центральную предметно-методическую комиссию.

1.3. Итоги регионального этапа подводятся отдельно по классам, победители и призеры регионального этапа определяются отдельно в каждом классе.

2. Порядок проведения соревновательных туров

2.1. Региональный этап олимпиады проводится в сроки, установленные Министерством просвещения Российской Федерации.

2.2. Время начала каждого тура регионального этапа олимпиады устанавливается в соответствии с расписанием регионального этапа, направляемым Министерством просвещения Российской Федерации, с учетом часовых поясов.

2.3. Региональный этап проводится в два тура: первый тур практический, второй тур проектный. Длительность практического тура составляет пять астрономических часов. Все участники регионального этапа должны быть допущены к участию в обоих турах, за исключением лиц, удаленных за нарушение Порядка проведения.

2.4. На каждом рабочем месте участника должны размещаться условия заданий и лист с логином и паролем для входа в тестирующую систему (если для авторизации используются логин и пароль). В распоряжение участников также должна предоставляться памятка участника, если она подготовлена жюри регионального этапа.

2.5. О начале тура объявляется по линии громкой связи или дежурными. Для оперативной координации во время тура дежурным по аудиториям, представителям жюри и оргкомитета, техническим специалистам разрешается использовать компьютеры, мобильные телефоны, планшеты, рации.

2.6. Участникам категорически запрещается перед началом и во время практического тура передавать свои логин и пароль другим участникам, пытаться получить доступ к

информации на компьютерах других участников или входить в тестирующую систему от имени другого участника.

2.7. В процессе практического тура участники имеют право задавать вопросы членам жюри по условиям задач. Вопросы должны задаваться в письменном виде на подготовленном жюри бланке. Если тестирующая система поддерживает возможность задавать вопросы, разрешается использовать эту функцию.

2.8. В случае если неоднозначность понимания условия приводит к многочисленным вопросам, жюри может сделать общее объявление для всех участников. Для консультации по условиям задач можно обращаться на горячую линию регионального этапа vos-ib@miem.hse.ru

2.9. В случае возникновения во время тура сбоев в работе компьютера или используемого программного обеспечения время, затраченное на восстановление работоспособности компьютера, может быть компенсировано по решению жюри, если сбой произошел не по вине участника.

2.10. Ответственность за сохранность своих данных во время тура каждый участник несет самостоятельно. Чтобы минимизировать возможные потери данных, участники должны своевременно сохранять свои файлы.

2.11. В случае если участник хочет досрочно завершить участие в туре, он может покинуть аудиторию только после согласования с оргкомитетом.

3. Регламент проведения проектного тура

3.1. Общие положения

3.1.1. Проект 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.

3.1.2. 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.

3.1.3. 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.

3.2. Направление проектной деятельности

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

3.2.2. 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.).

3.2.3. 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.

3.2.4. 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.

3.3. Критерии оценивания проектного тура

3.3.1. 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	2

Критерии оценки проекта			Баллы
		(полная – 2, частичная – 1, отсутствует – 0)	
	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
	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**

3.3.2 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**

Критерии оценки проекта			Баллы
	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
Оценка разработанного продукта 10 баллов	**2**	**Оценка продукта**	**10**
	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**

3.4. Регламент защиты проекта

3.4.1. Защита проекта происходит в устном формате в виде постерной сессии.

3.4.2. Участник представляет плакат, на котором отображены актуальность проекта, ход и результаты выполнения проекта.

3.4.3. Жюри обходит участников постерной сессии – проектного тура и задает вопросы.

3.4.4. Жюри может задавать вопросы участнику в течение 15.

3.4.5. Пояснительные записки направляются в оргкомитет регионального этапа на электронную почту, которая публикуется на сайте регионального этапа не менее чем за 10 дней до проведения очного мероприятия.

3.4.6. Оргкомитет осуществляет кодирование пояснительных записок и передает их жюри для ознакомления и оценивания.

4. Практический тур

4.1. Вариант проведения практического тура регионального этапа на платформе исполнения заданий CTFd, развернутой локально

4.1.1. Для проведения практического тура организаторам необходимо развернуть сетевую и серверную инфраструктуру и проверить её работоспособность согласно приведенным ниже требованиям по материально-техническому обеспечению. В общем виде инфраструктура проведения включает сервер для платформы CTFd (автоматической тестирующей системы), компьютеры участников с установленным в виртуальном окружении ПО для решения задач, сетевую инфраструктуру с необходимыми правами доступа.

4.1.2. Для выполнения заданий необходимо скачать и развернуть на сервере (серверах) виртуальную машину администратора (с установленной автоматической тестирующей системой – Платформой CTFd) и участников (с установленной операционной системой с утилитами для решения практических задач).

4.1.3. Общее описание инфраструктуры практического тура

1. Доступ в сеть Интернет в аудиториях проведения для участников должен отсутствовать. Интернет-доступ допускается только на рабочих местах организаторов/жюри в отдельном изолированном контуре. Локальная сети должна быть проводной со скоростью передачи данных не менее 1 Гбит/с.

2. На ПК участника установлен гипервизор VirtualBox (или аналог при обеспечении работоспособности и функциональности).

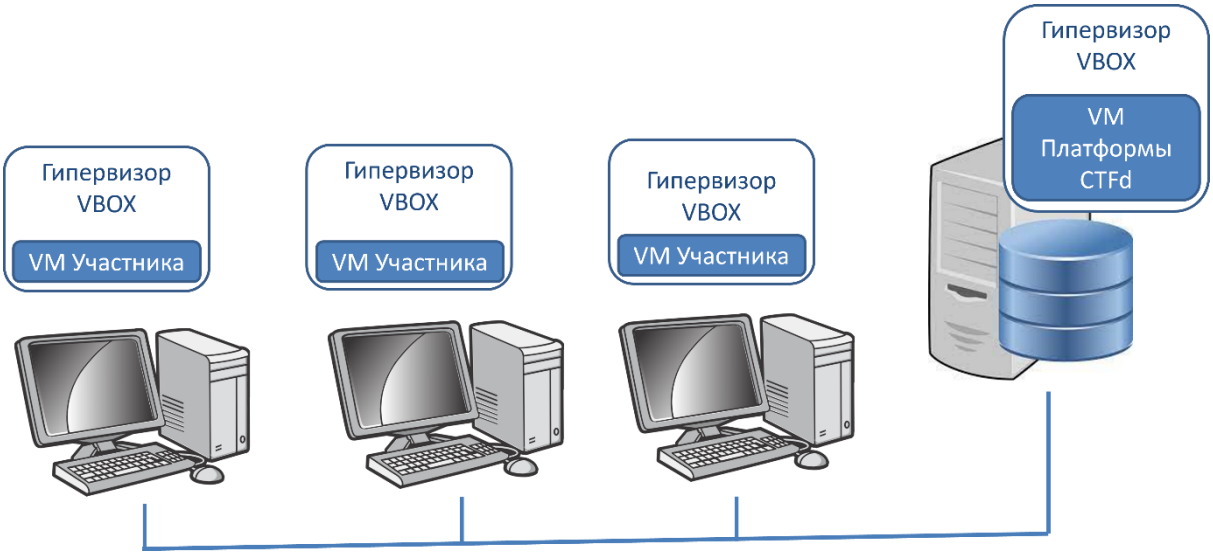
3. На Сервере установлен гипервизор VirtualBox (или аналог при обеспечении работоспособности и функциональности).

4. ПК участников и сервер организаторов доступны по сети.

5. Участнику предоставляется (установлен и работоспособен на момент начала практического тура) образ виртуальной машины с необходимым программным обеспечением для решения заданий. Виртуальную машину участника требуется запустить до начала практического тура.

6. На сервере администратора запускается виртуальная машина с Платформой с заданиями, которая используется для решения всех заданий. **Развертывание и проверка работоспособности Платформы производится заранее,** непосредственно организаторами, но не ранее чем за 4 дня до проведения практического тура. Виртуальная машина с Платформой (сервер) должна быть доступна по локальной сети с машин участников.

7. Для загрузки участниками файлов (скриншотов, скриптов, конфигурационных файлов и т.п.), подтверждающих выполнение заданий тематики СЗИ, организаторы предоставят механизм индивидуальной загрузки этих файлов (индивидуальные папки с персональным доступом для каждого участника или/и LMS).



8. Инструкции по настройке виртуальной машины администратора предоставляется на публичных ресурсах (vsosh.miem.hse.ru и другие)

4.2. Вариант проведения практического тура централизованно на облачной платформе CTFd

4.2.1. В 2025/26 гг. практический тур может (для ограниченного числа регионов) проходить в пилотном (тестовом) режиме с использованием централизованной облачной инсталляции CTFd. Регистрация и рассылка учётных данных выполняются региональным оператором через утверждённые формы сбора. Каждому участнику выдаётся уникальная пара логин/пароль для доступа к CTFd.

4.2.2. Для обеспечения равных условий вводятся синхронизированные временные окна с учётом часовых поясов и возможностью проведения в разные слоты для различных регионов (расписание публикуется региональным оператором, аутентификация активируется только в пределах регионального окна).

4.2.3. Подключение к облачной платформе происходит с использованием VPN и далее, аналогично локальному варианту по протоколу HTTPS. Инструкции по подключению направляются в регионы председателям жюри регионального этапа Олимпиады.

4.2.4. Если площадка не может использовать облачную платформу по техническим причинам, то после обоснования причин, организаторам может быть разрешено развернуть локальный образ CTFd. В этом случае (см. п. 4.1 требований, конфигурации будут аналогичны и/или идентичны облачной версии, но регистрация участников переходит под контроль региональной площадки. Результаты проведения олимпиады загружаются по установленной процедуре.

4.2.5. В случае тура централизованного проведения на облачной платформе площадка обязана предоставить участникам рабочие места с предустановленной виртуальной машиной, выдаваемой организаторами, аналогично обычному (локальному) варианту.

4.2.6. Интернет для участников разрешён исключительно для установления VPN-соединения с облачной платформой. Доступ к другим ресурсам сети Интернет и в локальной сети должен быть запрещен средствами сетевого администрирования. Нужно учитывать, что у участников есть неограниченные привилегии в выдаваемом образе виртуальной машины.

4.2.7. Организаторы обеспечивают стабильный сетевой канал по VPN предварительное тестирование подключения и мониторинг доступности. Необходимо проверить доступность и работоспособность соединения с VPN-сервером и Платформой не позднее чем 5 дней до даты проведения этапа.

4.2.8. Необходимость смены провайдера услуг связи, обеспечения стабильного и бесперебойного подключения находится исключительно в зоне ответственности региональных организаторов.

4.3. Процедура кодирования (обезличивания) и декодирования выполненных олимпиадных заданий практического тура

4.3.1. Поскольку проверка решений на олимпиаде по информатике проводится автоматически тестирующей системой, необходимости в обезличивании и декодировании выполненных заданий на олимпиаде по информатике нет.

4.3.2. При использовании облачной CTFd идентификация осуществляется встроенными аккаунтами платформы, дополнительных процедур обезличивания не требуется. Для локальных площадок требуется сопоставление рабочих мест с аккаунтами CTFd в протоколе обезличивания.

5. Критерии и методика оценивания выполненных олимпиадных заданий

5.1. В силу специфики задач олимпиады, проверка и оценивание решений практической части происходит с использованием средств Платформы (автоматической тестирующей системы). Участники отправляют решения на проверку во время тура, результаты проверки сообщаются участникам по мере готовности.

5.2. Итоговая оценка за выполнение заданий определяется путём сложения суммы баллов, набранных участником за выполнение заданий практического тура и защиты проекта.

5.3. Проект оценивается из 30 баллов в соответствии с критериями, указанными в пункте 3.3.

5.4. Практический тур оценивается из 70 баллов. Система оценивания конкретных заданий указывается в условиях задач соответствующего тура.

6. Требования по сохранению и предоставлению для последующей перепроверки результатов выполнения участниками регионального этапа в случае проведения практического тура регионального этапа на платформе CTFd

6.1. Для выборочной перепроверки результатов работ участников организаторы практического тура регионального этапа должны предоставить в ответ на запрос ЦПМК следующую информацию:

1. По всем участникам: снимок экрана платформы Scoreboard (Страница с результатами, пример на рис. 1)
2. По каждому участнику: список и содержание всех файлов, предоставленных участниками, в т.ч. для заданий категории СЗИ и Анализ трафика в виде архива .zip ИЛИ снимков экрана (пример на рис. 3 и 4). Список и содержание файлов этих категорий предоставляются на каждого участника.

6.2. Все перечисленные данные должны быть сохранены сразу после окончания выполнения участниками заданий практического тура. Отсутствие данных соответствует факту фальсификации результатов практического тура.

6.3. При проведении этапа с использованием централизованной облачной платформы, региональными организаторами предоставляются только те файлы/данные, что не загружаются на централизованную облачную платформу.

6.4. Для выполнения вышеуказанных требований после проведения Олимпиады (перед началом проверки) для оценки результатов участников, Организаторы должны выполнить снимок экрана платформы Scoreboard (Страница с результатами, пример на рис. 1) платформы CTFd (платформы для проведения практического тура). Снимок экрана

подтверждает факт выполнения заданий Олимпиады и позволяет проверить результаты участников.

Данные колонки 1 (Place, номера рабочих мест) должны соответствовать реальным рабочим местам участников на площадке проведения и подтверждаться протоколом обезличивания, с явным сопоставлением ФИО (или уникального идентификатора участника, при наличии) и номера рабочего места (id). В колонке Score находятся баллы участника, набранные на платформе.

Расшифровка колонок таблицы Scoreboard (Страница с результатами)

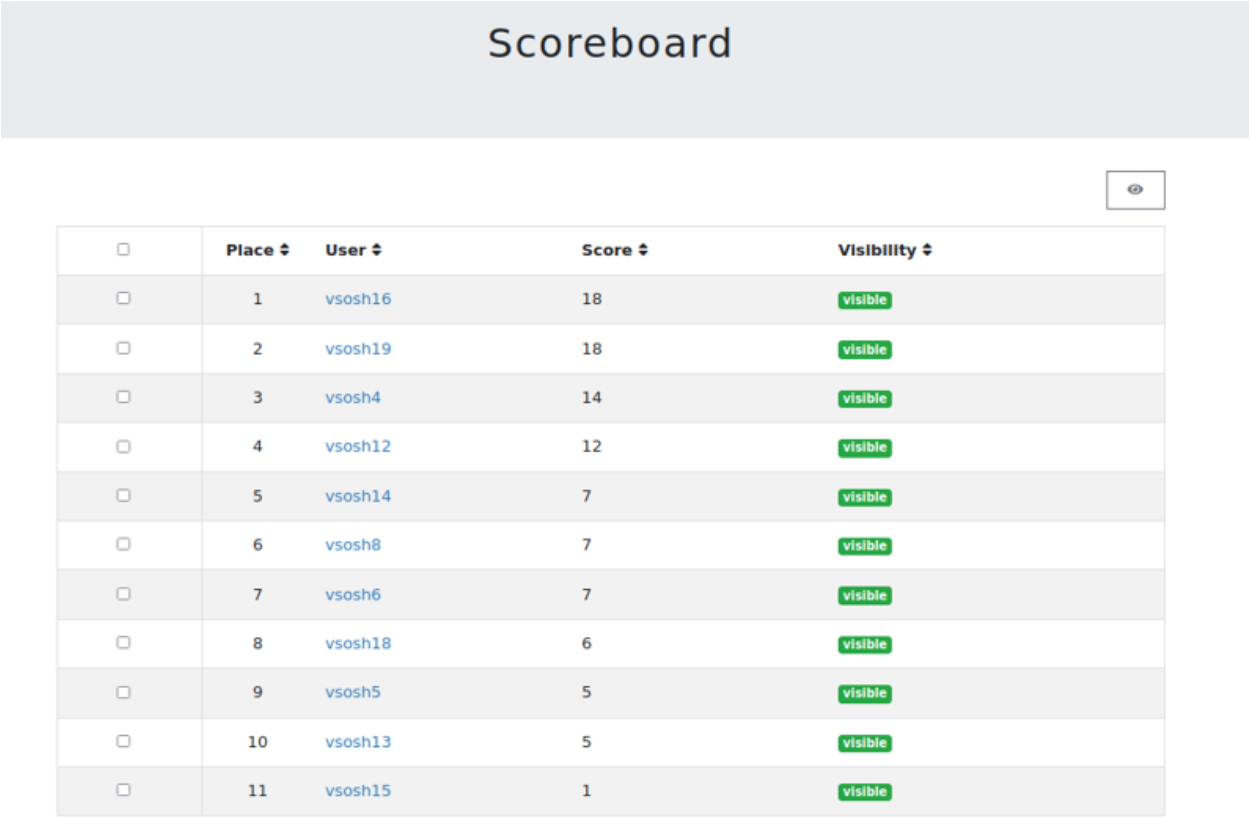
Place – id, номер рабочего места

User – имя пользователя на Платформе

Scor – число набранных баллов на Платформе

Visibility – видимость пользователя

Данные раздела Scoreboard (Страница с результатами) и должны совпадать данными участников в бланк-протоколе. Страница с результатами (Scoreboard) должна быть приложена к бланк-протоколу после окончания проверки.



	Place	User	Score	Visibility
☐	1	vsosh16	18	visible
☐	2	vsosh19	18	visible
☐	3	vsosh4	14	visible
☐	4	vsosh12	12	visible
☐	5	vsosh14	7	visible
☐	6	vsosh8	7	visible
☐	7	vsosh6	7	visible
☐	8	vsosh18	6	visible
☐	9	vsosh5	5	visible
☐	10	vsosh13	5	visible
☐	11	vsosh15	1	visible

Рисунок 1. – Страница с результатами Scoreboard (пример), которую необходимо сохранить и предоставить в ЦПМК при выборочной проверке (перепроверке) результатов участников.

Ссылка на страницу Scoreboard (Страница с результатами), которую необходимо зафиксировать снимком экрана находится в верхней части веб-интерфейса.

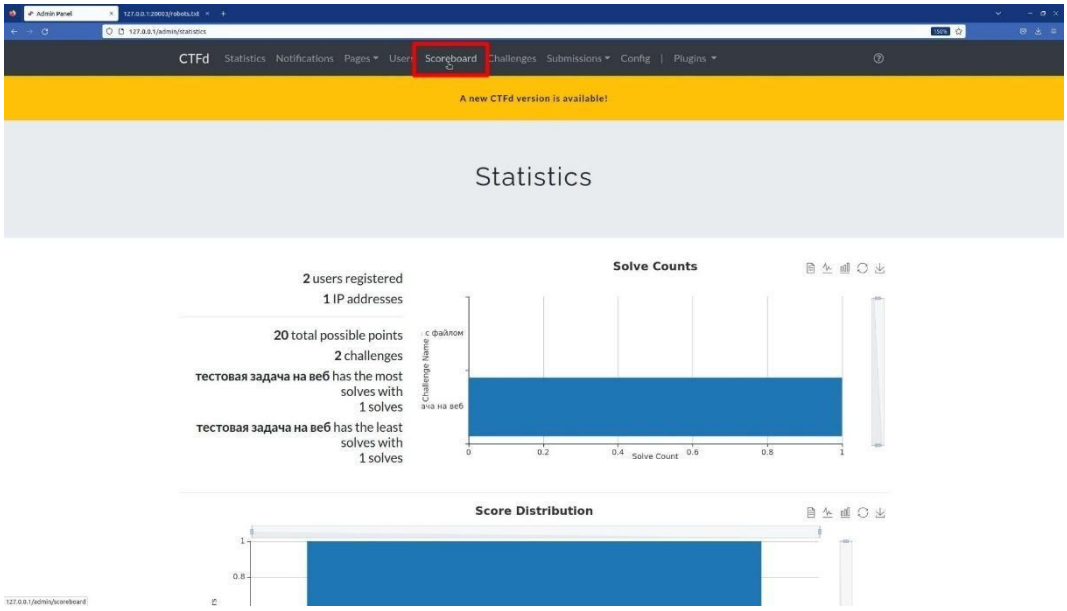


Рисунок 2. – Ссылка на страницу Scoreboard (обозначена красным прямоугольником)

6.5. Данные (списки и содержание всех загружаемых участником файлов, вне зависимости от способа загрузки – через LMS или CTFd) должны быть сохранены после окончания Олимпиады для последующей проверки и перепроверки в виде архива .zip ИЛИ снимков экрана (пример — на рис. 3 и 4). Список и содержание файлов этих категорий предоставляются на каждого участника.

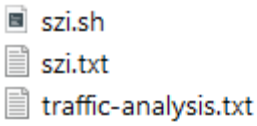


Рисунок 3. – Список файлов для участника N. Предоставляется на каждого участника с указанием рабочего места для каждого скриншота ИЛИ в виде электронного архива с файлами

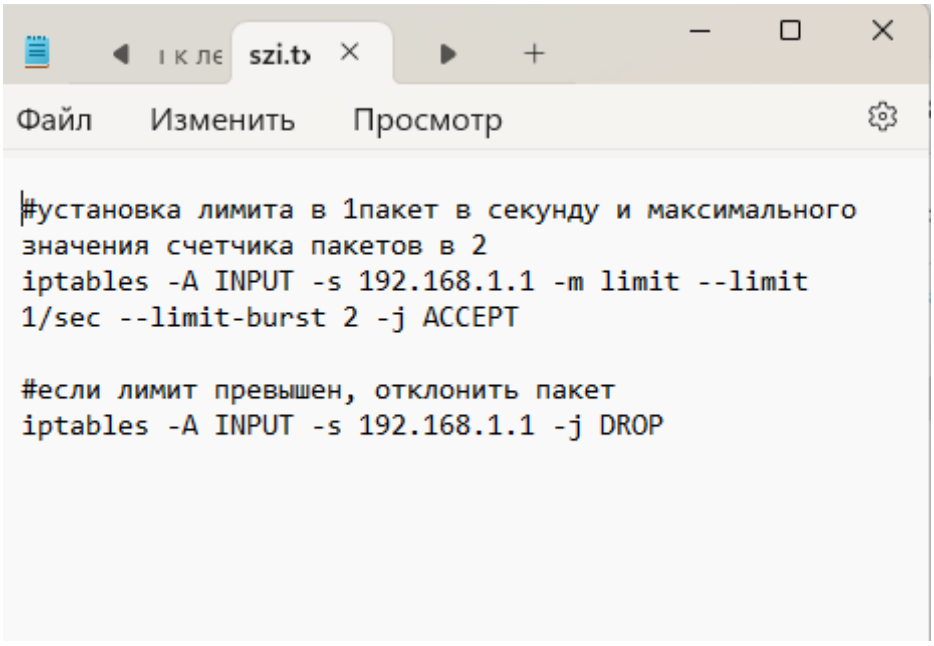


Рисунок 4. – Содержание одного файла для участника N. Предоставляется в виде снимка экрана каждого файла на каждого участника ИЛИ в виде электронного архива с файлами

Все перечисленные данные должны быть сохранены сразу после окончания выполнения участниками заданий практического тура.

7. Перечень материально-технического обеспечения для проведения регионального этапа

7.1. Общие требования

7.1.1. В качестве аудиторий для выполнения практических работ по профилю «Информационная безопасность» лучше всего подходят мастерские и кабинеты информатики (в расчете на 20 рабочих мест), в которых оснащение и планировка рабочих мест создают оптимальные условия для проведения этого этапа. При числе участников более 20 вычислительные мощности серверного оборудования должны быть линейно увеличены, обеспечивая возможность проведения олимпиады. На каждого участника должен быть предусмотрен персональный компьютер (ПК участника) с доступом в локальную сеть. В локальной сети должен быть предусмотрен отдельный компьютер (сервер организаторов), на который организован доступ по локальной сети с компьютеров участников. Сервер должен иметь выход в Интернет. Также предусмотрен резервный сервер. Системные требования, подключение к сети и состав ПО полностью аналогичны основному серверу. Резервный сервер используется при выходе из строя основного.

7.1.2. На ПК участника установлен монитор виртуальных машин (гипервизор) VirtualBox (или аналог при подтверждении работоспособности и функциональности). Участнику предоставляется образ виртуальной машины с необходимым программным обеспечением для решения заданий. Доступ в Интернет с машин участников категорически запрещен.

7.1.3. Все компьютеры участников и сервер организаторов должны иметь статические IP-адреса.

7.1.4. На сервере организаторов запускается виртуальная машина с Платформой (CTFd или аналог) с заданиями. Она используется для решения всех практических заданий, кроме заданий по работе с СЗИ (при наличии таких заданий). Для загрузки участниками файлов (скриншотов, скриптов, конфигурационных файлов и т.п.), подтверждающих выполнение заданий тематики СЗИ, должен быть организован механизм индивидуальной загрузки этих файлов. Например, через LMS, Яндекс-формы, общие папки на сервере (индивидуальные папки с персональным доступом для каждого участника).

7.1.5. Рабочие места участников должны быть изолированы друг от друга с помощью средств сетевого администрирования (ACL, VLAN или др.). При этом участники должны иметь доступ к центральному серверу (компьютеру организаторов по локальной сети).

7.1.6. В аудитории для организаторов и членов жюри должна быть доступна WiFi сеть не ниже 802.11n, с защищенным доступом (WPA2 или выше). Доступ к сети посторонних (других преподавателей, участников, экспертов и т.п.) должен быть запрещен. Доступ в Интернет с машин участников должен быть запрещен.

7.1.7. Для облачного варианта на рабочих местах участников разрешаются только VPN-концентратор и домен/адрес облачной CTFd (allow-list на L3/L7); доступ в Интернет в остальную часть сети запрещён.

7.1.8. Не позднее чем за день до проведения олимпиады организаторы проверяют и настраивают (при необходимости) сетевую инфраструктуру, разворачивают итоговую версию виртуальной машины на сервере организаторов, устанавливают средства мониторинга сетевого трафика для предотвращения прямого сетевого доступа между рабочими станциями участников олимпиады.

7.1.9. Организаторы обязаны проверить работоспособность функциональность Платформы CTFd (автоматической тестирующей системы) и других используемых систем (например, LMS) на региональной сетевой инфраструктуре не позднее чем за сутки до начала этапа. И в случае обнаружения проблем своевременно и устранить.

7.2. Особенности проведение при доступе к облачной Платформе CTFd

7.2.1. Площадка обязана предоставить участникам рабочие места с

предустановленной виртуальной машиной, выдаваемой организаторами аналогично обычному варианту.

7.2.2. Интернет для участников разрешён исключительно для установления VPN-соединения с облачной платформой. Доступ к другим ресурсам сети Интернет и в локальной сети должен быть запрещен средствами сетевого администрирования. Нужно учитывать, что у участников есть неограниченные привилегии в выдаваемом образе виртуальной машины.

7.2.3. Организаторы обеспечивают стабильный сетевой канал по VPN предварительное тестирование подключения и мониторинг доступности. Необходимо проверить доступность и работоспособность соединения с VPN-сервером и Платформой не позднее чем 5 дней до даты проведения этапа.

7.2.4. Необходимость смены провайдера услуг связи, обеспечения стабильного и бесперебойного подключения находится исключительно в зоне ответственности региональных организаторов.

7.3 Проверки Платформы CTFd

7.3.1. Как в случае локального развертывания Платформы, так и при облачном сценарии проведения, организаторы обязаны проверить функциональность платформы (автоматической тестирующей системы) CTFd с рабочих мест участников.

7.3.2. План тестирования для проверки заданий CTFd приведен в таблице ниже.

№ п/п	Тест	Плановый результат
1	Доступность Платформы с машин участников по протоколу HTTS	Платформа CTFd доступна с виртуальных машин участников (kali)
2	Доступ к платформе для тестовых пользователей, вход в систему, доступность заданий. Пользователей необходимо самостоятельно создать на Платформе или использовать штатных тестовых пользователей (не административную учетную запись)	Пользователи одновременно с разных компьютеров (виртуальных машин участника) могут войти в систему CTFd, успешно проходит авторизация, связь стабильная, есть доступ, задания доступны для скачивания и запуска
3	Запуск заданий, одновременно одно и тоже задание, не менее 3-х тестовых пользователей с различных компьютеров	Задания запускаются, к запущенным заданиям есть доступ согласно инструкции/текста задания
4	Запуск заданий, одновременно различные задания, не менее 3-х тестовых пользователей с различных компьютеров	Задания запускаются, к запущенным заданиям есть доступ согласно инструкции/текста задания
5	Скачивание файлов (задания на реверс и т.п.)	Файлы скачиваются
6	Повторный запуск заданий, одновременно одно и тоже задание, не менее 3-х тестовых	Задания запускаются, к запущенным заданиям есть доступ согласно

№ п/п	Тест	Плановый результат
	пользователей с различных компьютеров	инструкции/текста задания
7	Для всех участников есть учетные записи в CTFd	Для всех участников есть учетные записи в CTFd

7.4. Список необходимого оборудования и программного обеспечения

Практический тур по информационной безопасности		
№ п/п	Название	Кол-во, ед. измерения
1.	Сервер (компьютер) организаторов с доступом в локальную сеть (без выхода в Интернет) со следующими характеристиками: процессор не менее Intel i7, 12 ядер, RAM 64 Гбайт, SDD не менее 1000 Гбайт. USB-клавиатура и мышь в комплекте	1 шт. на каждые 20 участников. При числе участников более 20 серверные мощности (процессор, память и т.п.) должны быть линейно увеличены или должны быть развёрнуты дополнительные сервера исходя из числа 1 сервер на 20 человек
2.	Резервный сервер (компьютер) организаторов с доступом в локальную сеть (без выхода в Интернет) со следующими минимальными характеристиками: процессор не менее Intel i7, 8 ядер, RAM 64 Гбайт, SDD не менее 1000 Гбайт. USB-клавиатура и мышь в комплекте	1 шт.
3.	Персональный компьютер или ноутбук (ПК) с доступом в локальную сеть (без выхода в Интернет) со следующими минимальными характеристиками: процессор не менее Intel i5, 6 ядер, RAM 16 Гбайт, SDD не менее 500 Гбайт. USB-клавиатура и мышь в комплекте	На каждого участника, 1 шт.
4.	Монитор, не менее 24 дюймов (или экран ноутбука)	На каждого участника и сервер организаторов, не менее 1 шт.
5.	Установленный на ПК гипервизор (VBOX)	На каждого участника, не менее 1 шт.
6.	Виртуальная машина (Linux) с необходимым программным обеспечением для решения заданий (предоставляется организаторами)	На каждого участника, не менее 1 шт.
7.	Виртуальная машина с Платформой с заданиями, устанавливаемая на сервере организаторов (предоставляется организаторами в день соревнований)	1 шт. (в случае централизованного проведения на облачной платформе не требуется)
8.	Резервные рабочие места: персональный компьютер или ноутбук (ПК) с выходом в	2 шт. на каждые 20 человек

Практический тур по информационной безопасности		
№ п/п	Название	Кол-во, ед. измерения
	локальную сеть (без выхода в Интернет) со следующими характеристиками: процессор не менее Intel i5, 6 ядер, RAM 16 Гбайт, SDD не менее 500 Гбайт. USB-клавиатура и мышь в комплекте.	
9.	Локальная сеть Ethernet UTP (проводная), скорость не менее 1 Гбит/с	На учебный класс
10.	Доступ в Интернет с рабочего места организаторов (проводной, Ethernet UTP)	На учебный класс
11.	Доступ в Интернет по WiFi (защищенная сеть, версии WPA2 или выше)	Только для организаторов и членов жюри
12.	LMS-система для индивидуальной загрузки результатов выполнения заданий (файлов, скриншотов) или аналог	На учебный класс, с индивидуальным доступом по логину/паролю на участника
13.	Удаленный доступ по VPN к централизованной облачной платформе	Для варианта проведения на централизованной облачной платформе