

Оценивание проекта

Информация с рубриками-цифрами приведена из «Требований...»

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 (*постер-плакат*) 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 (ТТР) 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.

3.4.1. 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.

Пояснительная записка

Пояснительная записка должна быть оригинальной и отражать содержание и ход выполнения проекта. В пояснительной записке рекомендуется привести информацию об актуальности проекта, аналогах разработки, ее достоинствах. Особое внимание рекомендуется уделить ходу выполнения проекта путем отражения структуры проекта, основных разработанных элементах, отладке и тестированию проекта. Несомненным достоинством пояснительной записки будет приведенная информация о реальном использовании проекта.

Требования к оригинальности формально не предъявляются, как и требования по использованию систем с «искусственным интеллектом» (больших языковых моделей). При использовании материалов, полученных с использованием систем искусственного интеллекта и материалов других авторов должны быть указаны источники заимствований в соответствии с действующими стандартами. При обнаружении некорректных заимствований проект может быть снят с защиты.

Постер

Презентационный материал – постер представляет собой плакат формата А0 или А1 горизонтального или вертикального расположения, на котором распечатана информация о проекте. На плакате должна быть предоставлена вся информация, необходимая для оценивания. Обязательно на плакате должен быть размещен шифр участника, присвоенный организаторами этапа.

На постере не должно быть информации, раскрывающей школу/регион и ФИО участника и/или учителя/тренера/ментора. Оргкомитет этапа должен после размещения постеров на стенах и перегородках проверить отсутствие указанной информации.

Для постерной сессии рекомендуется использовать аудитории с возможностью крепления плакатов, размещения столов для установки компьютеров (стационарных или ноутбуков), раздаточных материалов и/или разработок, стула для участника. Рекомендуется не менее двух квадратных метров на участника.

Члены жюри (рекомендуемое количество – не менее 5 квалифицированных специалистов) могут как в составе группы, так и по одиночке подходить к участникам в произвольном порядке. Участнику предлагается сделать доклад до 5 минут по проекту, затем член(ы) жюри до 15 минут задают вопросы, направленные на обоснованное заполнение шаблона оценки (см. критерии оценивания проектного тура). Допускается, что другие участники проектного тура могут слушать вопросы члена(ов) жюри и ответов

участника, но не могут участвовать в беседе. Не допускается членами жюри доведения до участника информации об оценке проекта, однако могут быть высказаны рекомендации по развитию проекта.

Общая оценка членов жюри по проекту может рассчитываться допустимыми статистическими методами экспертного оценивания (расчета среднего, с учетом отбрасывания крайних значений, медианы и пр.).

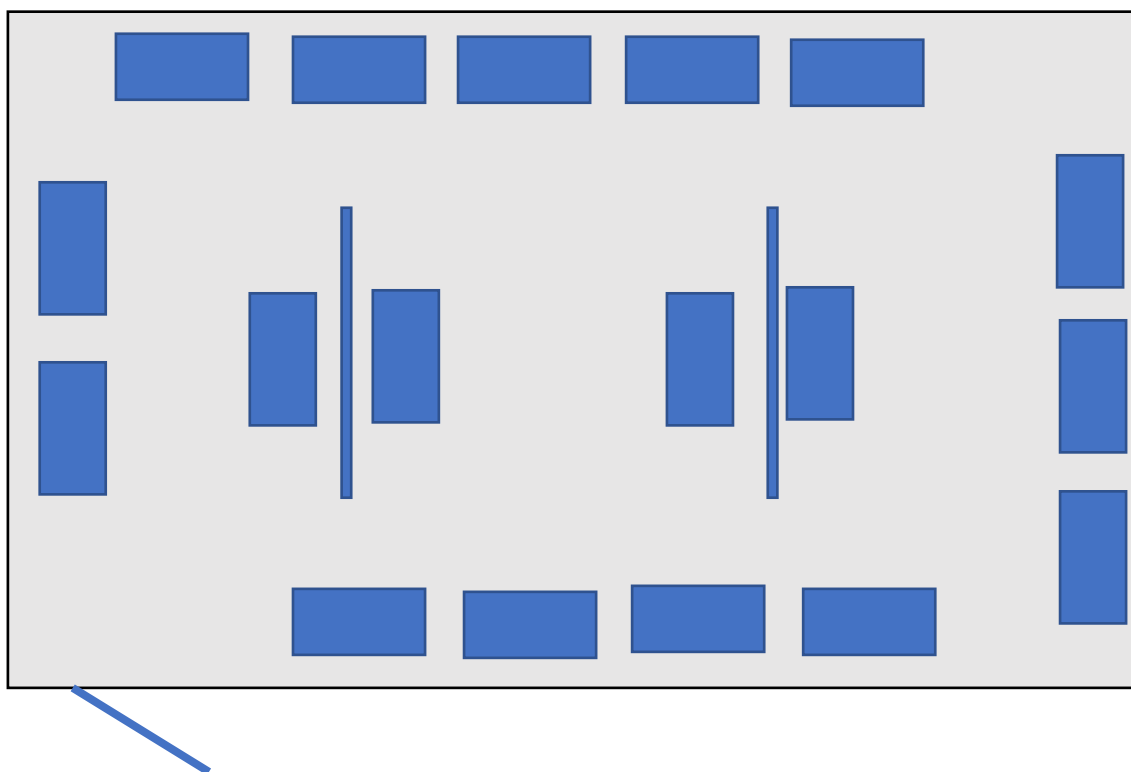
При большом количестве участников допускается размещение участников в различных аудиториях и создание нескольких потоков постерных сессий. Время нахождения участников в аудитории не должно превышать допустимого времени для соответствующего возраста участника. Рекомендуется ограничить одну постерную сессию 2-3 часами, включая время на монтаж и демонтаж постеров-плакатов, настройку компьютеров и иные действия.

При наличии возможности обеспечить участников презентационным оборудованием (телевизоры, проекторы, умные доски и пр.) допускается замена плаката аналогичной по формату презентацией.

Вариант размещения информации на плакате:

Наименование проекта		шифр
Актуальность	Аналоги	
Структура проекта	Особенности проекта	
Внедрение и тестирование	Перспективы развития проекта	
Общие выводы по проекту		

Вариант размещения постеров в аудитории



Синие прямоугольники – места участников – стол/стул и, при необходимости, компьютер или личная разработка

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 (полная – 2, частичная – 1, отсутствует – 0)	2
	2.2	Качество исполнения и новизна	4

Критерии оценки проекта			Баллы
	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 (высокая – 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
	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

Критерии оценки проекта			Баллы
	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 (ТТР) 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